НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»

ФАКУЛЬТЕТ ПРИКЛАДНОЇ МАТЕМАТИКИ

Кафедра системного програмування і спеціалізованих комп‘ютерних систем

«До захисту допущено»

Завідувач кафедри
_____ Віталій РОМАНКЕВИЧ

“___” червня 2020 р.

Дипломний проект

на здобуття ступеня бакалавра

за освітньо-професійною програмою «Комп’ютерні системи та компоненти»

зі спеціальності **123 «Комп'ютерна інженерія»**

на тему: Система забезпечення надійності транзакцій з використанням технології блокчейн

Виконала: студентка IV курсу, групи КВ-61
(шифр групи)

Коркішко Анастасія Олександрівна _____
(прізвище, ім’я, по батькові) (підпис)

Керівник доц. каф. СПіСКС к.т.н., доцент Орлова М.М. _____
(посада, науковий ступінь, вчене звання, прізвище та ініціали) (підпис)

Консультант з нормоконтролю, доц.каф.СПСКС, к.т.н. Клятченко Я.М.

(назва розділу) (посада, вчене звання, науковий ступінь, прізвище, ініціали) (підпис)

Рецензент _____
(посада, науковий ступінь, вчене звання, науковий ступінь, прізвище та ініціали) (підпис)

Засвідчую, що у цьому дипломному проекті немає запозичень з праць інших авторів без відповідних посилань.
Студент _____
(підпис)

Київ – 2020 року

НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»

ФАКУЛЬТЕТ ПРИКЛАДНОЇ МАТЕМАТИКИ

Кафедра системного програмування і спеціалізованих комп'ютерних систем

Рівень вищої освіти – перший (бакалаврський)

Спеціальність 123 «Комп'ютерна інженерія»

Освітньо-професійна програма «Комп'ютерні системи та компоненти»

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ Віталій РОМАНКЕВИЧ
(підпис) (ініціали, прізвище)
«__»_____20___р.

ЗАВДАННЯ
на дипломний проєкт студента

Коркішко Анастасія Олександрівна

1. Тема проєкту «Система забезпечення надійності транзакцій з використанням технології блокчейн»,

керівник проєкту доц. каф. СПіСКС к.т.н., доцент Орлова М.М.,

затверджені наказом по університету від «__»_____20__р. №_____

2. Термін подання студентом проєкту 22.05.2020

3. Вихідні дані до проєкту Система забезпечення надійності транзакцій з використанням технології блокчейн.

4. Зміст пояснювальної записки
   1. Аналіз існуючих методів транзакцій
   2. Аналіз проблеми надійності Blockchain
   3. Технологія Blockchain
   4. Смарт контракт
   5. Порівняння роботи консенсусів Proof of work та Proof of Stake

6. Створення приватного blockchain
7. Створення смарт контракту
8. Тестування смарт контракту

5. Перелік графічного матеріалу (із зазначенням обов'язкових креслеників, плакатів, презентацій тощо): структура блоків у мережі Blockchain. Схема структурна; схема проведення транзакцій у криптовалютах на основі технології блокчейн. Схема структурна; алгоритм проведення транзакцій у мережі Blockchain. Схема структурна. Принцип взаємодії основних модулів проведення транзакції. Схема структурна.

6. Консультанти розділів проєкту*

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
нормоконтроль	Ярослав КЛЯТЧЕНКО		

7. Дата видачі завдання 10.09.2019

Календарний план

№ з/п	Назва етапів виконання дипломного проєкту	Термін виконання етапів проєкту	Примітка
1.	Вивчення літератури за тематикою проекту	11.10.2019	
2.	Розроблення та узгодження технічного завдання	24.10.2019	
3.	Аналіз існуючих рішень	16.01.2020	
4.	Підготовка матеріалів першого розділу дипломного проєкту	09.03.2020	
5.	Підготовка матеріалів другого розділу дипломного проєкту	28.03.2020	
6.	Підготовка матеріалів третьої частини дипломного проєкту	25.04.2020	
7.	Оформлення документації дипломного проєкту	05.05.2020	
8.	Попередній огляд матеріалів диплому на кафедрі	21.05.2020	

Студент _____ _Анастасія КОРКІШКО___
Керівник проєкту _____ _Марія ОРЛОВА____

_____

АННОТАЦІЯ

Кваліфікаційна робота включає пояснювальну записку (59 с., 34 рис., 3 табл., список використаної літератури з 12 найменувань, 3 додатки).

Метою бакалаврського дипломного проєкту є аналіз надійності технології blockchain та розроблення приватного blockchain для підвищення надійності грошових переказів та написання смарт контракту для виконання фінансових транзакцій всередині приватного blockchain.

Для досягнення даної мети був проведений ретельний аналіз переваг та недоліків технології blockchain, дослідження різновидності смарт контрактів та способи їх написання, порівняння принципів роботи proof of work та proof of stake, порівняння їх діяльності.

В результаті було розроблено приватний blockchain та написано смарт контракт для реалізації фінансових транзакцій. Протестовано роботу смарт контракту та продемонстровано результати його роботи в дипломному проєкті.

Розроблений приватний блокчейн та смарт контракт можна успішно використовувати в фінансових структурах для грошових переказів між користувачами.

Ключові слова: блокчейн, смарт контаркт, proof of work, proof of stake, транзакція.

SUMMARY

Qualification work includes an explanatory note (59 pages, 34 figures, 3 tables, list of references from 12 items, 3 appendices).

The aim of the bachelor's thesis project is to analyze the reliability of blockchain technology and develop a private blockchain, to increase the reliability of money transfers and write a smart contract to perform financial transactions within a private blockchain.

To achieve this goal, a thorough analysis of the advantages and disadvantages of blockchain technology, a study of the variety of smart contracts and ways to write them, a comparison of the principles of proof of work and proof of stake, a comparison of their activities.

As a result, a private blockchain was developed and a smart contract was written to implement financial transactions. The work of the smart contract was tested and the results of its work in the diploma project were demonstrated.

The developed private blockchain and smart contract can be successfully used in financial structures for money transfers between users.

Keywords: blockchain, smart contact, proof of work, proof of stake, transaction.

Поз.	Формат	ПОЗНАЧЕННЯ	НАЙМЕНУВАННЯ	Кількість аркушів	№ прим.	Примітки
1	А4	ІАЛЦ.045440.002 ТЗ	Система забезпечення	4		
			надійності транзакцій з			
			використанням технології			
			Blockchain.			
			Технічне завдання			
2	А4	ІАЛЦ.045440.003 ТП	Система забезпечення	2		
			надійності транзакцій з			
			використанням технології			
			Blockchain.			
			Відомість технічного			
			проекту			
3	А4	ІАЛЦ.045440.004 ПЗ	Система забезпечення	59		
			надійності транзакцій з			
			використанням технології			
			Blockchain.			
			Пояснювальна записка			
4	А4	ІАЛЦ.045440.005 Д1	Система забезпечення	1		
			надійності транзакцій з			
			використанням технології			
			Blockchain.			
			Структура блоків у мережі			
			Blockchain.			

Змін.	Арк.	№ докум.	Підпис	Дата	**ІАЛЦ.045440.001 ОА**		
Розробив		Коркішко А.О.			*«Система забезпечення надійності транзакцій з використанням технології блокчейн»*	Літ.	Аркуш 1 / Аркушів 3
Керівник		Орлова М.М.					
Н. контроль		Клятченко Я.М.			***Опис альбому***	***НТУУ «КПІ ім. Ігоря Сікорського», ФПМ, КВ-61***	
Зав. каф.		Романкевич В.О.					

Поз.	Формат	ПОЗНАЧЕННЯ	НАЙМЕНУВАННЯ	Кількість аркушів	№ прим.	Примітки
			Схема структурна			
5	А4	ІАЛЦ.045440.006 Д1	Система забезпечення	1		
			надійності транзакцій з			
			використанням технології			
			Blockchain.			
			Схема проведення			
			транзакцій у			
			криптовалютах на основі			
			технології блокчейн.			
			Схема структурна			
6	А4	ІАЛЦ.045440.007 Д1	Система забезпечення	1		
			надійності транзакцій з			
			використанням технології			
			Blockchain.			
			Алгоритм проведення			
			транзакцій у мережі			
			Blockchain.			
			Схема структурна			
7	А4	ІАЛЦ.045440.008 Д1	Система забезпечення	1		
			надійності транзакцій з			
			використанням технології			
			Blockchain.			
			Принцип взаємодії			
			основних модулів			

Поз.	Формат	ПОЗНАЧЕННЯ	НАЙМЕНУВАННЯ	Кількість аркушів	№ прим.	Примітки
			проведення транзакції.			
			Схема структурна			
8		Диск CD-ROM	Текст пояснювальної	1		
			записки.			
			Графічні матеріали			

Зміст

1. НАЙМЕНУВАННЯ І ОБЛАСТЬ ЗАСТОСУВАННЯ

Найменування роботи – «Система забезпечення надійності транзакцій з використанням технології блокчейн».

Область застосування: Використання смарт-контракту для виконання грошових транзакцій між користувачами.

2. ПІДСТАВА ДЛЯ РОЗРОБКИ

Підставою для розробки є завдання на виконання роботи першого (бакалаврського) рівня вищої освіти, затверджене кафедрою системного програмування і спеціалізованих комп'ютерних систем Національного технічного університету України «Київський Політехнічний Інститут імені Ігоря Сікорського».

3. ЦІЛЬ І ПРИЗНАЧЕННЯ РОБОТИ

Метою даного проекту є аналіз надійності технології Blockchain та розробка приватного блокчейну та написання власного смарт контракту для виконання транзакцій.

4. ДЖЕРЕЛА РОБОТИ

Джерелами роботи є науково-технічна література з технології blockchain, написання смарт контрактів; електронні статті у мережі Internet, що стосуються цих питань.

5. ТЕХНІЧНІ ВИМОГИ

5.1. Вимоги до апаратного забезпечення:

- Комп’ютер на базі процесора Intel Core
- Оперативна пам’ять - 1024 Мбайт і більше.
- Наявність доступу до мережі Internet.

5.2. Вимоги до програмного забезпечення:

- Операційна система Windows, Linux, OS X.
- Середовище REMIX.
- ПлатформаGETH.
- Гаманець «Mist».
- Internet-браузер (Google Chrome, Safari, Internet Explorer або інший).

5.3. Функціонал програмного забезпечення:

- можливість користування власним приватним блокчейном для підвищення надійності транзакцій.
- Можливість управління грошима.
- Переказ коштів між учасниками.
- Можливість купувати та продавати монети
- Визначення можливостей учасників.

6. ЕТАПИ РОЗРОБКИ

№ з/п	Назва етапів виконання дипломного проєкту	Термін виконання етапів проєкту	Примітка
1.	Вивчення літератури за тематикою проекту	11.10.2019	
2.	Розроблення та узгодження технічного завдання	24.10.2019	
3.	Аналіз існуючих рішень	16.01.2020	
4.	Підготовка матеріалів першого розділу дипломного проєкту	09.03.2020	
5.	Підготовка матеріалів другого розділу дипломного проєкту	28.03.2020	
6.	Підготовка матеріалів третьої частини дипломного проєкту	25.04.2020	
7.	Оформлення документації дипломного проєкту	05.05.2020	
8.	Попередній огляд матеріалів диплому на кафедрі	21.05.2020	

Поз.	Формат	ПОЗНАЧЕННЯ	НАЙМЕНУВАННЯ	Кількість аркушів	№ прим.	Примітки
	А4	ІАЛЦ.045470.004 ПЗ	Система забезпечення	59		
			надійності транзакцій з			
			використанням технології			
			Blockchain.			
			Пояснювальна записка			
	А4	ІАЛЦ.045470.005 Д1	Структура блоків у мережі	1		
			Blockchain.			
			Схема структурна			
	А4	ІАЛЦ.045470.006 Д1	Схема проведення	1		
			транзакцій у			
			криптовалютах на основі			
			технології блокчейн.			
			Схема структурна			
	А4	ІАЛЦ.045470.007 Д1	Алгоритм проведення	1		
			транзакцій у мережі			
			Blockchain.			
			Схема структурна			

Змін.	Арк.	№ докум.	Підпис	Дата	ІАЛЦ.045470.003 ТП		
Розробив		Коркішко А.О.			Система забезпечення надійності транзакцій з використанням технології блокчейн **Відомість технічного проекту**	Літ.	Аркуш 1 / Аркушів 1
Перевірив		Орлова М.М					
Консульт.						КПІ ім. Ігоря Сікорського, ФПМ КВ-61	
Н. контроль		Клятченко Я.М.					
Зав. каф.		Романкевич В.О.					

Поз.	Формат	ПОЗНАЧЕННЯ	НАЙМЕНУВАННЯ	Кількість аркушів	№ прим.	Примітки
	А4	ІАЛЦ.045470.008 Д1	Принцип взаємодії	1		
			основних модулів			
			проведення транзакції.			
			Схема структурна			
		Диск CD-ROM	Текст пояснювальної	1		
			записки.			
			Графічні матеріали.			

Змін.	Арк.	№ докум.	Підпис	Дата	ІАЛЦ.045470.003 ТП	Арк. 2

ЗМІСТ

Перелік скорочень, умовних позначень, термінів

Bitcoin	–	це цифрова валюта, створена в січні 2009 року.
Blockchain	–	розподілена книга транзакцій, яка дублюється і розподіляється по всій мережі комп'ютерних систем на blockchain.
Смарт-контракт	–	самовиконуваний договір, умови між покупцем і продавцем якого записуються прямо в рядки коду.
Proof of work	–	система, яка прикладає зусилля для того, щоб стримувати легковажні чи зловмисні використання обчислювальної потужності.
Proof of stake	–	концепція, яка зазначає, що людина може видобувати чи підтверджувати нові блокові транзакції відповідно до того, скільки монет вона має.
Solidity	–	об'єктно-орієнтована мова програмування для написання смарт контрактів.
Ethereum	–	децентралізована програмна платформа з відкритим кодом, що використовується для власної криптовалюти, ефіру.

ВСТУП

Життя сучасного суспільства нерозривно пов’язане з грошима, документами та інформацією. Коли починаєш думати про гроші, то відразу уявляєш купу монет чи банкнот, проте насправді більшість грошей стали віртуальними досить давно. Та насправді, технології зайшли далі, тому що вже кілька років доступні нові види цифрових валют. Їх називають криптовалютами та віртуальними валютами. Головною мотивацією до створення такого виду грошей є децентралізація фінансів. Саме це і призвело до винаходу технології Blockchain. Цей термін виник в контексті Bitcoin. Це технологія цифрової валюти, яка була винайдена та опублікована в інтернеті у 2009 році анонімною особою або групою осіб. Оскільки, ця технологія ще досить молода, то вона досі розвивається стрімкими темпами. Є переконання, що Bitcoin має великий потенціал та може призвести до кардинальних змін в економічній, правовій та політичній сферах.

Залежно від контексту термін Bitcoin може мати декілька наступних значень.

1) Додаток Bitcoin – це програмне забезпечення з відкритим кодом, яке можна використовувати на власному комп’ютері. Воно не належить людині чи компанії, а його розробкою та підтримкою займається громада добровільних розробників [1].
2) Мережа Bitcoin – це відкрита група комп’ютерів, які спілкуються на основі раніше визначених правил (протоколу).
3) Цифрова валюта Bitcoin – це одиниця вартості, яка генерується, захищається та відстежується комп’ютерами мережі.

Проте, Bitcoin - це цифрова валюта з досить сумнівною безпекою. Найбільші ризики пов'язані з архітектурними параметрами його Blockchain. Зокрема, відсутня можливість зупиняти, відкликати або піддавати цензурі транзакції. На додачу до всього, відсутня будь-яка схема страхування.

Таким чином, Blockchain – це структура даних, яка використовується Bitcoin-ами або подібним додатком для публічного запису історії транзакцій з цифровою валютою, список записів, кількість яких постійно збільшується, що називають блоками, які пов’язані за допомогою криптографії. Кожен блок містить криптографічний хеш попереднього блоку, часову позначку та дані транзакцій (як правило, представлені у вигляді дерева) [1].

Blockchain розподіляється серед однорангових мереж і управляється ними. Оскільки це розподілений регістр, то він може існувати без централізованого управління. Дані про блочний ланцюг групуються в блоки. Після цього блоки з’єднуються один з одним і захищаються з використанням криптографії.

Blockchain – це постійно зростаючий список записів. Його структура створена так, що дані можливо тільки додавати в базу даних, змінити чи видалити раніше введені дані на попередніх блоках неможливо. Саме тому Blockchain підходить для запису подій, ведення записів, обробки транзакцій, відслідковування активів та голосування.

З розвитком технології Blockchain почали розвиватись контракти, побудовані на комп’ютерних алгоритмах, і отримали назву смарт-контракти. Смарт-контракт - це самостійно виконуючий договір, умови якого описано безпосередньо в рядках коду, який контролює виконання угоди, а транзакції відстежуються та є незворотними. Смарт-контракти дозволяють здійснювати транзакції та угоди серед анонімних сторін без необхідності центрального органу, правової системи чи зовнішнього механізму. Незважаючи на те, що технологія Blockchain вважається в основному призначеною для Bitcoin, вона розвинулася далеко за межами віртуальної валюти. Нік Сабо, американський вчений, який винайшов віртуальну валюту під назвою «Біт Голд» у 1998 році, визначив смарт-контракти як комп’ютеризовані протоколи транзакцій, які виконують умови контракту. Вони надають можливість транзакції бути простежуваною, прозорою та незворотньою.

Окрім ефективності, Blockchain має й інші унікальні характеристики, які роблять його проривним нововведенням. Blockchain вважається надійним, оскільки повну копію книги Blockchain підтримують усі активні вузли. Таким чином, якщо один вузол переходить в автономний режим, книга все ще буде доступна для всіх інших учасників мережі. Крім того, кожен блок ланцюга посилається на попередні блоки, що запобігає видаленню або зміни транзакцій після їх додавання до Blockchain. Отже, цілісність і надійність мережі залишатимуться недоторканими до тих пір, поки вона використовується. Ця мережа є децентралізованою, тобто ніхто не контролює Blockchain і не може змінювати його [1].

1. АНАЛІЗ ІСНУЮЧИХ РІШЕНЬ ТА ОБҐРУНТУВАННЯ ТЕМИ ДИПЛОМНОГО ПРОЕКТУ

1.1. Аналіз актуальності задачі

Вплив криптовалюти продовжує рости на фоні того, що курси різних валют все підвищуються. За роки існування криптовалюти її майбутнє було предметом суперечок фахівців, багато з яких вважали, що незабаром вона втратить свою актуальність. Однак, з різким зростанням вартості Bitcoin і появою перших криптомілліардерів, стало очевидно, що поширення електронного золота триватиме, а разом з ним продовжить змінюватися і світова економіка, а розмови про заборону або обмеження використання нового ресурсу в різних країнах перестали виникати.

Ринок криптовалюти в останні кілька років продовжує бурхливо рости. Найбільш відомою і дорогою грошовою одиницею залишається всім відомий Bitcoin, якому належать лаври першопрохідця і революціонера на світових ринках. Максимальна кількість Bitcoin-ів налічує близько 21 млн штук, і значна частина валюти поки що не розподілена і не «здобута», що означає, що Bitcoin ще довго не вичерпає свій потенціал. Однак валют зараз вже дуже багато, і їх кількість і вартість буде зростати [2].

Однією з нових валют з сильними позиціями на світових ринках є Ethereum - валюта на базі Blockchain, що створюють сервери, що не мають центру і працюють у вигляді смарт-контрактів. Ця валюта з'явилася зовсім недавно, але вже зараз отримує неформальний статус електронної нафти. Багато фахівців вважають, що ця валюта стане дорожче Bitcoin вже в найближчі роки.

Blockchain технології в союзі з розвитком криптовалюти на їх основі мають величезний потенціал розвитку і впливу на світову економіку. Створення нової національної криптовалюти в рамках окремої країни, за розрахунками Банку Англії, дасть державі додаткові 3% приросту ВВП. Також варто

відзначити, що технологія транзакцій і розподілу криптовалюти володіє величезними функціями і можливостями. Придбання валют на увазі практично криптографічний реєстрацію прав власності. Суб'єкт, який володіє валютою, стає автоматичним власником власності. Право власності суб'єкта допоможе застовпити все той же Blockchain. Таким чином, даний алгоритм може застосовуватися і до приписку криптовалюта вартості звичайних грошових коштів на ринку. Це робить криптовалюту електронним аналогом грошей звичайних, при цьому криптовалюта залишається універсальною, прозорою і зручною, тобто зберігаючи всі плюси криптовалюта. У зв'язку з цим варіант того, що криптовалюта буде витісняти звичайну валюту, бачиться цілком можливим [2].

1.2. Аналіз існуючих методів транзакцій

Транзакція – процес проведення угоди або заключення договору. Походить від латиського слова transactio, яке означає узгодження. Найголовніше, що транзакція не може бути виконана наполовину або чверть. У даного поняття є лише 2 стани – або виконано, або ні, наче в комп’ютерній логікі – 0 або 1. Отже, це логічно завершена операція, наскільки довгою вона не була та зі скількох етапів вона не складалася б [3].

1.2.1. Аналіз банківських транзакцій

Найрозповсюдженішим типом до недавнього часу була банківська транзакція – будь-яка дія, яка спричинила собою зміну стану рахунку клієнта банку. Це може бути і простий переказ з одного рахунку на інший, і зняття грошей з картки в банкоматі, і оплата карткою в магазині.

Складність процедури традиційної банківської онлайн транзакції полягає в наступному.

За допомогою POS-терміналу, з метою аутентифікації власника, інформація про карту з терміналу передається в банк-еквайрер, який обслуговує даний термінал, і має угоду з власником торгової точки. Залежно

від домовленостей торгова точка оплачує банку комісію за його участь в обробці транзакції. Далі банк-еквайрер передає інформацію в платіжну систему, яка обслуговує дану карту. Там дані потрапляють в операційний центр, до якого підключені банки-учасники платіжної системи. У цьому центрі проходить перевірка на предмет наявності або відсутності платіжних даних карти в стоп-аркуші і в залежності від отриманого результату в транзакції відмовляється або вона схвалюється з подальшим спрямуванням до банку-емітента, що випустив дану карту, і обслуговуючий прив'язаний до неї банківський рахунок / рахунки клієнта. Тут вона потрапляє в процесинговий і авторизаційний центр, в якому проводяться розширені перевірки на легальність оброблюваної транзакції. При підозрі на шахрайство або порушення умов обслуговування дається відмова. Залежно від типу карти (дебетова або кредитна) і встановленого банком пріоритету авторизації тут може проводитися перевірка доступного залишку коштів на рахунку або платіжного ліміту, а також звірятися авторизаційний PIN-код власника. При задоволенні всім перевіркам емітент схвалює операцію і в рамках транзакції, також через платіжну систему, відповідь дається в торгову точку. Шляхом взаєморозрахунків з платіжною системою емітент перераховує еквайреру суму запитуваних по транзакції коштів, а також комісію платіжної системи за обробку транзакції. У свою чергу з клієнтського рахунку банк списує оплачувану і підтверджену клієнтом до оплати суму грошей (для дебетових карт) або зменшує доступний платіжний ліміт, тим самим резервуючи частина коштів до подальшого списання (для кредитних карт). Транзакція завершується в момент надходження назад в торгову точку відповіді зі схваленням чи відмовою.

1.2.2. Аналіз транзакцій в базах даних

Сучасний СУБД (Система Управління Бази Даних) є розрахованою на багато користувачів. Отже, завжди є можливість одночасного звернення

кількох користувачів до однієї бази даних, і навіть - до одних і тих самих даних. При цьому виникає маса проблем, пов'язаних зі спробами одночасної зміни або видалення даних.

Транзакція - послідовний набір команди SQL, який утворює логічно завершений блок, який виконується як єдине ціле. У транзакції може бути включена від однієї до кількох тисяч команд [4]. Управління транзакцією засновано на вимогах ACID:

- автономність;
- послідовність;
- ізоляція;
- довговічність.

Управління потребами ACID працює завдяки серверу. Розробник повинен вибрати необхідний рівень ізоляції та розробити ефективні алгоритми обробки даних. Для кожної транзакції сервер додає до даних блокування, які створюють виконання вимог ACID. Блокування (замок) - тимчасово накладається обмеження використання декількох операцій для обробки даних. До складу СУБД, як правило, входить менеджер блокування, який управляє блокуванням. У разі відсутності механізму блокування виникають такі ситуації: (р - окремий кортеж таблиці):

1) проблема останньої зміни (the lost update problem) представлена в таблиці 1.1.

Зміни, виконані транзакціями А і В будуть загублені. Причиною «простоїв» при виконанні транзакцій В і С може бути, наприклад, їх старт з віддалених комп'ютерів мережі, або очікування в транзакції введення користувача.

Таблиця 1.1 – Приклад проблеми останньої зміни

	Транзакція A	Транзакція B	Транзакція C
T1	Взяти p	Взяти p	Взяти p
T2	Змінити p	-	-
T3	-	Змінити p	-
T4	-	-	Змінити p

2) Проблема «брудного» читання (the uncommitted dependency problem)

Таблиця 1.2 – Приклад «брудного» читання

	Транзакція A	Транзакція B
T1	Взяти p	-
T2	Змінити p	Взяти p
T3	Змінити p	-

Транзакція B буде зчитувати дані, можливо, які знаходяться в неузгоджену стані, викликаному тривалою транзакцією A і великою кількістю змін в транзакції A.

3) Проблема неповторюваного читання (the inconsistent analysis problem)

Таблиця 1.3 – Приклад неповторюваного читання

	Транзакція A	Транзакція B
T1	Взяти p	Взяти p
T2	-	Змінити p
T3	Взяти p	-

Дані, зчитані транзакцією А в перший раз, можуть відрізнятися від даних, зчитаних нею вдруге, тому що в цей час транзакція В встигла змінити ці дані.

Для вирішення зазначених проблем американським інститутом стандартів ANSI був розроблений стандарт на рівні блокування, що складається з наступних чотирьох рівнів [4].

- Рівень 0 - заборона даних (no trashing of data).

  Змінювати дані здатна тільки єдина транзакція. Якщо інша транзакція має намір змінити ці ж дані, вона має чекати, поки перша транзакція не завершить свою роботу.
- Рівень 1 - заборона на «брудну» читання (no dirty reads).

  Якщо транзакція початку змінила дані, то жодна інша транзакція не може читати ці ж дані, поки вони використовуються пешою транзакцією.
- Рівень 2 - заборона неповторюваного читання (no nonrepeatable reads).

  Якщо транзакція зчитує дані, то ніяка інша транзакція не зможе їх змінити. Таким чином, при повторному читанні даних вони будуть знаходитися в початковому стані.
- Рівень 3 - заборона фантомів (no phantom).

  Якщо транзакція звертається до даних, то ніяка інша транзакція не зможе додати / видалити рядки, які можуть бути зчитані при виконанні.

Рівень 0 є найслабшим обмеженням на одночасне звернення до даних. Рівень 3 - найжорсткіший, але, відповідно, і гарантує максимальну надійність. Рішення про те, який рівень блокування застосувати, приймає менеджер блокування конкретної СУБД, проте програміст має можливість задавати потрібний рівень блокування для конкретної транзакції, і навіть для конкретної команди SQL.

1.2.3. Аналіз Bitcoin -транзакцій

Blockchain Bitcoin є ланцюжком блоків, який включає публічну базу з інформацією про всі транзакції з Bitcoin, тобто передачі BTC від одного адресата іншому [5]. Кожен елемент ланцюга блоків мережі Blockchain

зберігає: історію про попередні операції; інформацію про нові транзакції (рис. 1.1). Кожен елемент ланцюга блоків мережі Blockchain зберігає:

- історію про попередні операції;
- інформацію про нові транзакціях.

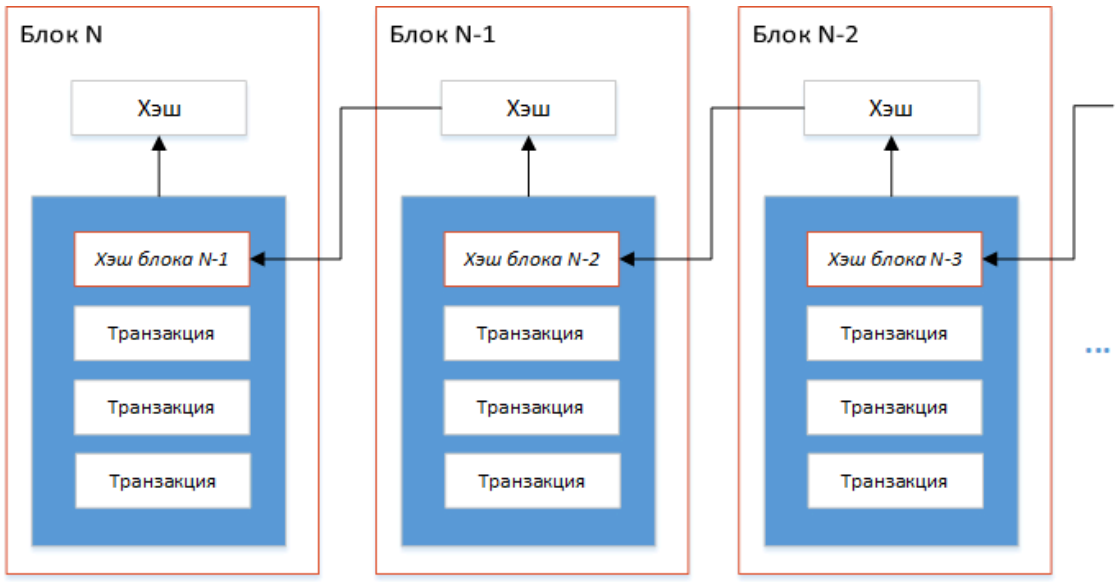

Рисунок 1.1 - Принцип формування блоків з даними про транзакції в мережі Bitcoin

Таким чином, Blockchain - це зв'язний список, в якому кожен наступний запис посилається на один попередній і так по ланцюжку до найпершої транзакції в мережі (рис. 1.2).

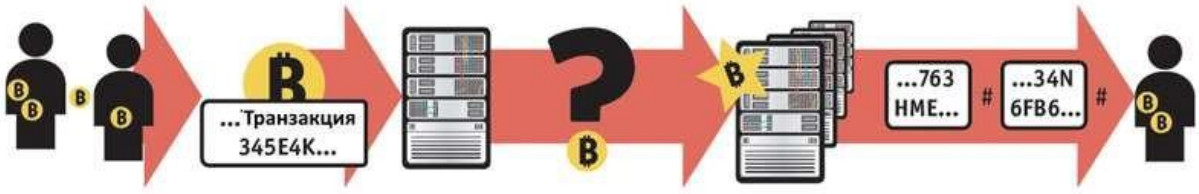

Рисунок 1.2 - Метод проводення Bitcoin-транзакцій в Blockchain Bitcoin

Проведення Bitcoin транзакцій відбувається в наступній послідовності [5].

1) Користувачі ініціюють Bitcoin-платіж, використовуючи спеціальне програмне забезпечення, так названі «гаманці».

2) Всі нові транзакції відправляються в глобальну мережу Bitcoin.
3) Приблизно кожні 10 хвилин комп’ютери, які входять глобальну мережу (майнери), об’єднують декілька сотень транзакцій в один «блок».
4) Майнери підтверджують нову транзакцію, тим самим легітимізуючи її
5) За свою роботу у вигляді затрачених обчислювальних потужностей майнери отримують нагороду у формі емітованих Bitcoin-ів.
6) Черговий блок додається в загальну базу транзакцій мережі Bitcoin (Blockchain).
7) Надходження нових коштів відобразиться в гаманці отримувача.

Інформація про операції з Bitcoin-ами записується в спеціальні блоки, які представляють собою список транзакцій. Якщо скласти блоки в ланцюжок, то отримаєте історію криптовалюти. Блок складається з заголовка і списку транзакцій. Тема містить хеш-коди транзакцій, власний і хеш попереднього блоку. Першою в списку йде транзакція, в якій вказується винагорода (комісія) за створення нового блоку. Щоб перевірити справжність операцій з криптовалютою, транзакції повинні бути завалідовані до Blockchain. Він являє собою розподілену БД. Її частини зберігаються на безлічі комп'ютерів в мережі Bitcoin. Підтвердження транзакції - це її приєднання до списку транзакцій в блоці. Після проведення операції з криптовалютою рахунки відправника і одержувача оновлюються не відразу. У традиційних користувальницьких додатках для підтвердження транзакції має бути знайдено шість блоків, які доводять її валідність. При цьому користувач, який проводить операцію, може зменшити число перевірок. Це слід робити, якщо оперуєте невеликою сумою Bitcoin-ів. Це спрощує і прискорює процес підтвердження транзакції. Якщо верифікації перекладу криптогрошей не відбулося, то система повертає кошти назад на гаманець відправника.

Аналіз часу транзакції в Blockchain Bitcoin

В середньому на транзакцію йде від 20 хвилин до 60 хвилин, але в моменти пікового навантаження цей час може бути збільшено у багато разів. Час

очікування залежить від завантаженості мережі Blockchain. За останні два роки кількість операцій з Bitcoin-ами зросла більш ніж в 8 разів. Це видно на графіку нижче (рис. 1.3).

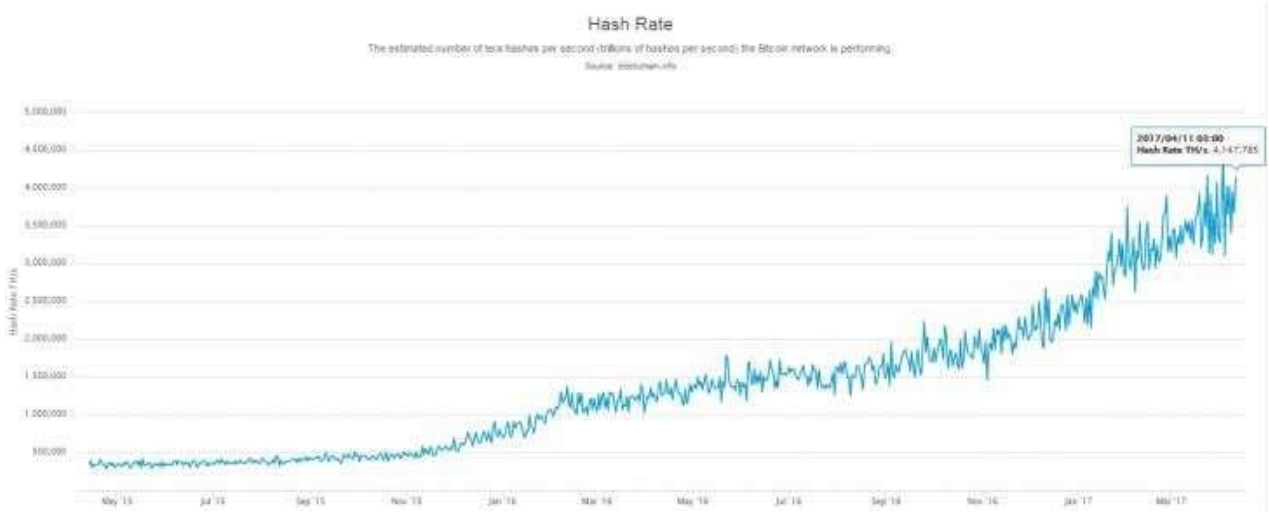

Рисунок 1.3 - Завантаженість мережі Bitcoin

Даний графік демонструє зростання кількості трильйонів хешів, які виконуються протягом декількох секунд в мережі Bitcoin. В мережі бувають несподівані підйоми, коли середня кількість транзакцій в блоках зростає, і розміри блоків досягають критичної межі.

Методи скорочення часу транзакції:

- підвищення плати Майнерам.

  Від 0,0002 BTC – мінімальна ціна, яку варто віддавати майнерам за підтвердження блоку.

- Обсяг переказаних коштів.

  Чим більше криптовалюти переводити, тим пріоритет операції підвищується в «криптомережі».

Аналіз різниці між підтвердженими та непідтвердженими транзакціями. Підтвердженням транзакції – це процес, коли транзакція додається до знайденого блоку. Той момент, коли підтверджень (включень в один) більше

ніж шість або більше, то транзакція є підтвердженою. Дана специфікація введена для захисту від повторної транзакції одних і тих же Bitcoin. Тобто, Bitcoin-клієнт буде бачити, що транзакція є «непідтвердженою» доки не накопичеться шість підтверджень (шість знайдених блоків). Сайти або сервіси, які працюються з Bitcoin для розразунку за товари або послуги, можуть вводити свої обмеження для кількості блоків,які є необхідними для підтвердження транзакції. Цифра шість є не випадковою, а грунтується на теорії: ймовірність того, що зловмисник зможе зібрати більше ніж десять відсотків від хешрейта мережі для підробки транзакцій, є малою, тому даний невеликий ризик (менший ніж 0,1%) є дозволеним.

1.2.4. Аналіз переваг Bitcoin транзакцій в порівнянні з банківськими тразакціями.

Список переваг Bitcoin-транзакцій в порівнянні з банківськими:

1) Нульові або дуже низькі комісії.

Комісії практично не залежать від переданої суми або від місця розташування відправника та отримувача. Найчастіше транзакції безкоштовні. Комісія необхідна лише при формуванні технічно великих транзакцій, які навантажують мережу, або дуже малих сум, щоб уникнути атаки на мережу за допомогою спаму величезної кількості безглуздих транзакцій.

Також відсутня будь-яка абонентська плата, ліміти та інші обмеження.

2) 27/7/365.

Переказ може бути відправлений коли завгодно, незалежно від часу, тому що в даної мережі немає вихідних.

3) Розширене покриття фінансовими послугами.

Різноманітність поточних платіжних систем так і не забезпечило повного територіального покриття та значного зниження витрат на грошові перекази. Особливо це стосується міжнародних переказів і невеликих сум. Наприклад, комісії за переказ 100 гривень може скласти 250 гривень. А в деяких країнах

Африки більш поширені платежі за допомогою мобільних телефонів і передплачених сервісів, ніж банківські послуги.

Для використання криптовалюти не потрібно використовувати дорогу інфраструктуру. У найпростішому випадку досить встановити легкий гаманець на свій смартфон і вже можна приймати і відправляти платежі. Це цілком достатня умова для охоплення тих соціальних верств, які не користуються на даний момент банківськими послугами.

При цьому немає поділу на міжнародні та місцеві платежі, вартість транзакції від цього не залежить. Можна навести аналогію з міжміським телефонним зв'язком і інтернет-месенджера типу Skype. Вони дозволяють здійснювати через Інтернет дзвінки значно дешевше, дозволяють проводити відео зв'язок, конференції та мають низку інших переваг. Аналогічно, електронне листування свого часу замінило традиційну паперову пошту. Так само і криптовалюта зараз починають замінювати деякі традиційні, але застарілі платіжні інструменти.

1.3. Аналіз проблеми надійності Blockchain

Існує багато різних напрямків, в яких можуть відбуватися атаки. Наприклад, зловмисник може вгадати персональні ключі і підписати фальшиві транзакції, щоб вкрасти Bitcoin. Інший шлях - ініціювати транзакції, які виглядають правильними і підтвердженими, в той час як обманутий відправник продовжує вважати, що вони були недійсними, і відповідні монети не витрачені. Ще один спосіб - спробувати вивести мережу з ладу за допомогою значних обчислювальних потужностей. Висококваліфіковані хакери можуть знаходити і нові, досі невідомі уразливості, і використовувати їх для компрометації інфраструктури Blockchain. Крім того, серйозні ризики для безпеки Bitcoin можуть представляти наступні сценарії [6]:

- Використання атак перебором (brute force) з метою підібрати персональні ключі для конкретних адрес.

- Отримання персонального ключа шляхом перебору по словнику.
- Повторне витрачання одних і тих же засобів за короткий проміжок часу.
- Виведення з ладу мережі.
- Використання вад протоколу.
- Використання недоліків криптографічної реалізації.

З одного боку, необхідність використовувати сторонні платіжні системи робить Bitcoin досить вразливим. З іншого боку, характеристики, властиві Bitcoin, забезпечують його більш досить високу надійність. До них можна віднести наступні [6].

- Транзакції є незворотніми.
- Транзакції не схильні до цензури.
- Адреса Bitcoin гаманця ніяк не пов'язана з правом власності на засоби.

Ці три пункти означають, що:

- Якщо людина втратить свій персональний ключ, то втратить і Bitcoin.
- Якщо людина зробите помилку при введенні адреси одержувача, то втратить Bitcoin.
- Якщо персональний комп'ютер буде зламаний, людина може втратити Bitcoin.
- Якщо персональний гаманець буде зламаний, людина втратить Bitcoin.
- Якщо буде зламана система безпеки використовуваної криптовалютної біржі, людина втратить власні Bitcoin.
- Крадіжка Bitcoin відбувається непомітно.

Таким чином, можна стверджувати, що Bitcoin далеко не такий надійний, як вважає більшість людей.

1.4. Формалізація постановки задачі дослідження

Задачею першого розділу бакалаврського проєкту є дослідження актуальності проблем, що стосуються забезпечення надійності транзакцій в Blockchain, оцінка існуючих методів проведення транзакцій.

Окрім того, метою даного дослідження є вивчення теоретичного підґрунтя описаних систем, проведення аналізу впливів різноманітних факторів, аналіз будови архітектури, технологій, платформ та існуючих рішень.

2. ТЕХНОЛОГІЯ BLOCKCHAIN. SMART CONTRACT. PROOF OF AND PROOF OF STAKE

2.1. Технологія Blockchain

2.1.1. Особливість технології Blockchain

В найпростішому значенні блокчейн представляє собою серію незмінних записів даних з мітками часу, якими управляє кластер комп'ютерів, які не належать якому одному суб'єкту. Кожен з цих блоків даних (тобто блок) захищений та пов'язаний один з одним за допомогою криптографічних принципів (тобто ланцюга)[7].

У чому його особливість та у чому саме він може призвести до небувалого покращення можливостей галузі?

1) Мережа блокчейн не має центрального управління – це і є визначення демократизованої системи. Оскільки це загальний та незмінний регістр, то інформація в ньому є відкритою для кожного. Отже, все що побудовано на блокчейні є максимально прозорим, і всі учасники несуть відповідальність за свої вчинки.
2) Блокчейн не несе транзакційних витрат. Це простий, але оригінальний спосіб передачі інформації від А до В повністю автоматизованим та безпечним способом. Одна сторона транзакції ініціює процес, створюючи блок. Цей блок буде перевірений тисячами, можливо, мільйонами комп'ютерів, які розподілені по мережі. Потім його додають в ланцюг, який зберігається в мережі, створюючи не просто унікальний запис, а з його власною історією. Фальсифікація одного запису буде означати фальсифікацію всього ланцюга мільйонами екземплярів. Це практично неможливо. Біткоїн використовує цю модель для грошових транзакцій, але її можна розгорнути багатьма іншими способами.

3) У фінансовому світі програми є більш очевидними, а революційні зміни – більш неминучими. Блокчейн змінить спосіб роботи фондових бірж, придбання позик та страхування. Вони ліквідують банківські рахунки та практично всі послуги, пропоновані банками. Практично кожна фінансова установа збанкрутує або змушена буде кардинально змінитись, коли технології будуть широко зрозумілі та впроваджені.

2.1.2. Основні принципи роботи технології Blockchain

Інформація, що зберігається на блокчейні, існує як спільна і постійно узгоджується – база даних. Це спосіб використання мережі, який має очевидні переваги. База даних блокчейн не зберігається в жодному місці, тобто записи, які вона зберігає, є справді загальнодоступними та легко перевіряються. Не існує централізованої версії цієї інформації, щоб злочинець міг змінити дані[7].

Причини, чому блокчейн завоював довіру:

1) Він не є власністю жодного суб'єкта, отже він децентралізований.
2) Дані криптографічно зберігаються всередині.
3) Блокчейн незмінний, тому ніхто не може підробляти дані, що знаходяться всередині блокчейна.
4) Блокчейн прозорий, тому можна відслідковувати дані.

Принципи, на яких будується робота технології Blockchain [7]:

- ☐ Децентралізація.

До появи біткоїна, більшість сервісів були централізованими. Тобто, є централізована організація, яка зберігає всі дані, і користувач має взаємодіяти виключно з цим об'єктом, щоб отримати будь яку необхідну інформацію (рис. 2.1).

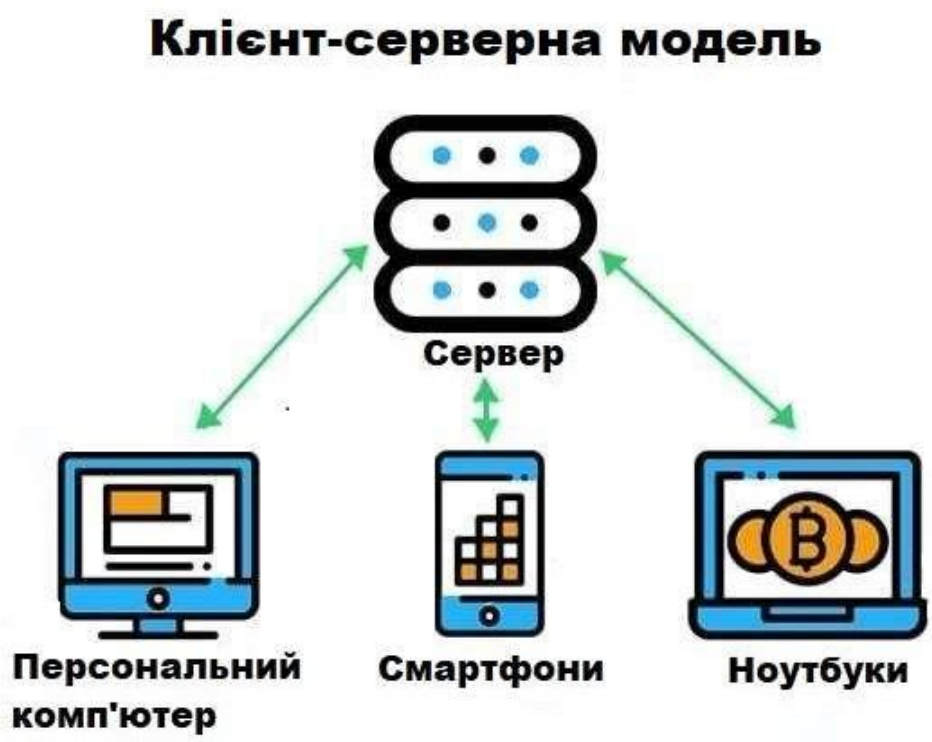

Рисунок 2.1 - Традиційна модель клієнт-сервер.

Проте у централізованих систем є недоліки:

1) Оскільки вони централізовані, то всі дані зберігаються в одному місці. Це робить їх легкою ціллю для потенційних хакерів.
2) Якщо централізований об’єкт по якихось причинах відключиться, то ніхто не зможе отримати доступ до інформації, якою він володіє.
3) Якщо об’єкт буде пошкоджено, то всі дані, які знаходяться всередині будуть порушені.

Різниця, якщо саме ця система була б децентралізована, полягає (рис. 2.2) [7].

Всі в мережі володіють інформацією.

Два комп’ютери можуть контактувати безпосередньо, не проходячи сторонніх шляхів. Це була основна ідеологія біткоїнів. Ви можете надсилати свої гроші будь-кому, не проходячи через банк.

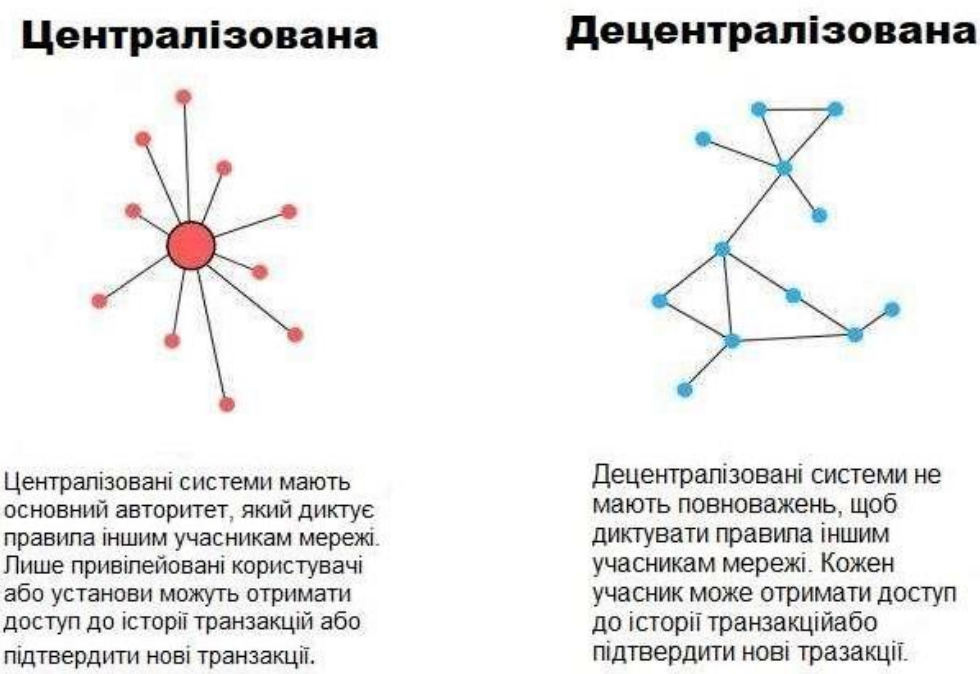

Рисунок 2.2 – Різниця між централізованою та децентралізованою мережею

☐ Прозорість

Особистість людини прихована за допомогою складної криптографії та представлена лише їх публічною адресою. Отже, якщо шукати історію транзакцій людини, то повідомлення буде виглядати «1MF1bhsFLkBzzz9vpFYEmvwT2TbyCt7NZJ відправив 1 BTC» (рис. 2.3).

TxHash	Block	Age	From	To	Value	[TxFee]
0x2d055e4585ae2a...	5629306	16 secs ago	0x003e3655090890...	0x2bdc9191de5c1b...	0,004741591554641 Ether	0.000294
0xb4d37c791ff4cde...	5629306	16 secs ago	0x6c3b4faf413e0e4...	0xf14cb3acac7b230...	0,744767225 Ether	0.000294
0x9979410dcb5f4c...	5629306	16 secs ago	0x99bcd75abbac05...	0x2d42ee86390c59...	0,016294 Ether	0.000294
0x189c4d4aae09be...	5629306	16 secs ago	0x175cd602b2a1e7...	0xd39681bb0586fb...	0,01 Ether	0.000294
0xda0e9bbb11fb77...	5629306	16 secs ago	0x73a065367d111c...	0x01995786f14357...	0 Ether	0.00150007
0x6be498fafad9acb...	5629306	16 secs ago	0xa3eb206871124a...	0x8a91cac422e55e...	0,029594 Ether	0.000294

Рисунок 2.3 - Знімок транзакцій Ethereum

В той час поки справжня особа людини захищена, все одно можна побачити всі транзакції, які були за адресою. Такого рівня прозорості не існувало в фінансовій системі до цього.

☐ Незмінність.

Незмінність в контексті блокчейн означає, що якщо колись щось було введено в блокчейн, це не може бути підроблене. Причина, чому блокчейн маю дану властивість – це функція криптографічного хеша.

Хешування, або хеш-функція – одна з основних складових сучасної криптографії та алгоритму блокчейна, використовується в багатьох алгоритмах і протоколах. Це особливе перетворення будь якого об'єма інформації, в результаті якого буде деяке відображення, образ, який називається хешем – унікальний короткий символьний рядок, який властивий тільки даному масиву вхідної інформації.

Отже, хеш має такі властивості, як:

1) Унікальність

Кожному набору (масиву) інформації притаманний суворо певний унікальний хеш. Проте іноді зустрічаються так звані колізії – випадки, коли хеш-функція для різних вхідних блоків інформації обчислює однакові хеш коди.

Математики-криптографи намагаються створити такі хеш-функції, ймовірність колізії в яких прагнула б до нуля [8]. Функцій, які обчислюють хеш, існує безліч. Найбільш поширена (зокрема використовується в протоколі блокчейна біткоїна) хеш-функція під назвою SHA-256 (від Secure Hash Algorithm - безпечний алгоритм хешування) (рис. 2.4). Ця хеш-функція формує хеш у вигляді рядка з 64 символів (довжина - 256 біт або 32 байта).

INPUT	HASH
Hi	3639EFCD08ABB273B1619E82E78C29A7DF02C1051B1820E99FC395DCAA3326B8
Welcome to blockgeeks. Glad to have you here.	53A53FC9E2A03F9B6E66D84BA701574CD9CF5F01FB498C41731881BCDC68A7C8

Рисунок 2.4 – Приклад хеш функції

2) При самій незначній зміні вхідної інформації її хеш змінюється кардинально.

Ця властивість дуже важлива при використанні хешування в цифровому підпису, тому що дозволяє упевнитися, що підписана інформація не була змінена під час її передачі по каналах зв'язку (рис. 2.5).

INPUT	HASH
This is a test	C7BE1ED902FB8DD4D48997C6452F5D7E509FBCDBE2808B16BCF4EDCE4C07D14E
this is a test	2E99758548972A8E8822AD47FA1017FF72F06F3FF6A016851F45C398732BC50C

Рисунок 2.5. – Приклад зміни хеш функції, при мінімальній змінівхідних данних

3) Хеш-функція необоротна

Не існує зворотної функції, яка з хеша може відновити вихідний масив інформації [8]. Відновити по хешу відповідний йому масив інформації можливо тільки перебором всіх можливих варіантів, що практично неможливо.

4) Висока швидкість роботи

Хешування дозволяє досить швидко обчислити шуканий хеш для досить великого масиву вхідної інформації. Цим хешування істотно відрізняється від кодування (шифрування) і декодування (дешифрування).

Блокчейн підтримується одноранговою мережею [9]. Мережа – сукупність вузлів, які з'єднані між собою. Вузли – це окремі комп'ютери, які приймають на вхід і виконують функцію на них і дають вихід. Блокчейн використовує особливий тип мережі під назвою «однорангова мережа», яка розподіляє все своє навантаження між учасниками, які однаково привілейовані. Немає одного центрального сервера, є кілька розподілених і децентралізованих учасників з рівними правами.

Одне з головних застосувань мережі учасників з рівними правами – це спільний доступ до файлів, який також називається торрент. Якщо використовувати для завантаження модель клієнт-сервер, вона як правило, надзвичайно повільна і повністю залежить від стану здоров'я сервера, також він схильний до цензури. Однак у системі peer-to-peer немає центральної інстанції, а отже, якщо навіть хтось із рівних учасників у мережі вийде з процесу, то є більше учасників для завантаження (рис. 2.6).

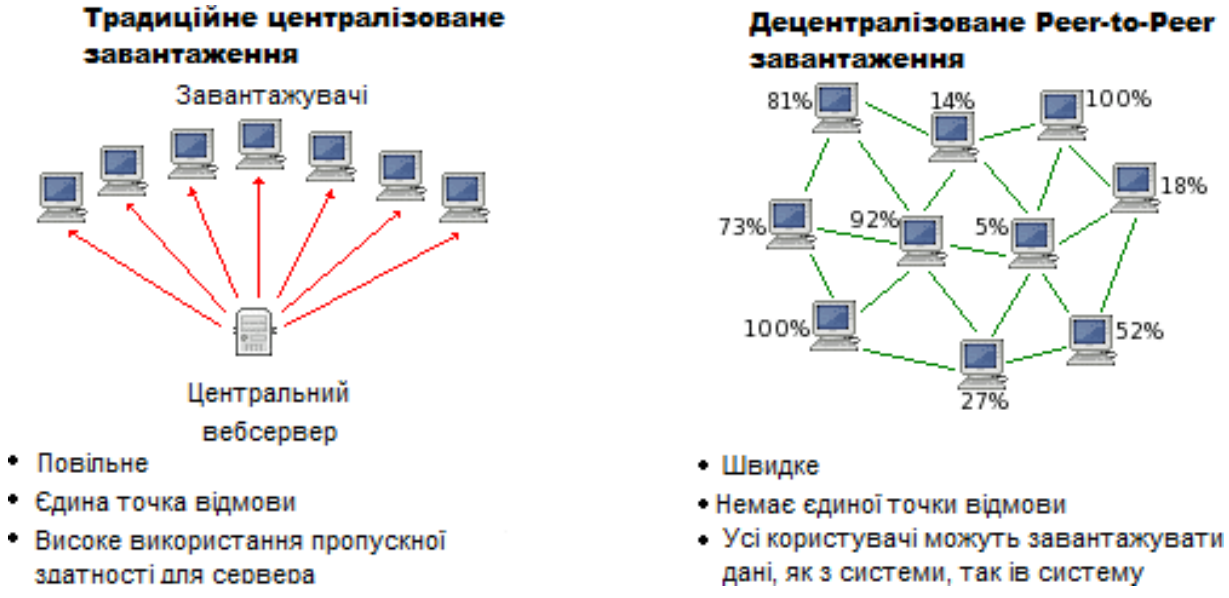

Рисунок 2.6 - Порівняння двох видів мережі

Однорангова мережа в криптовалюті структурована відповідно до механізму консенсусу, який використовується. Для криптовалют, таких як Bitcoin та Ethereum, які використовують звичайний механізм консенсусу на доказ роботи (Ethereum з часом перейде до Proof of Stake), усі вузли мають однакові привілейовані [9]. Основна ідея у створенні егалітарної мережі. Вузли не мають особливих привілегій, однак вони можуть мати різні функції та ступінь участі. Це має бути плоска топологія, без централізованого сервера або сутності, а також ієрархії.

Саме для того щоб криптовалюти залишались вірними своїй філософії, необхідно щоб вони були структуровані саме таким чином. Ідея полягає у створенні валютної системи, де всі члени будуть вважатись рівноправними, не буде існувати органу управління, який би міг диктувати вартість валюти.

Завдяки тому, що мережа дотримується gossip протоколу, система може існувати без центрального органу. Наприклад, один учасник надіслав іншому учаснику 3 ETH. Після цього, найближчі вузли дізнаються про це, і тоді вони повідомлять своїх «сусідів» про цю подію, і це буде продовжуватись до тих пір, поки кожен учасник системи не дізнається про цю подію.

Отже, вузол - це комп'ютер, підключений до мережі Blockchain. Вузол з’єднується з Blockchain за допомогою клієнта. Клієнт допомагає у валідації та розповсюдженні транзакцій на Blockchain. Підключаючись до Blockchain, його копія даних завантажується в систему, потім виконується синхронізація останнім блоком даних на Blockchain (рис. 2.7).

Є три види участі в мережі [9].

- Зберігаючи неглибоку копію blockchain
- Зберігаючи повну копію blockchain
- Перевіряючи транзакції (Mining)

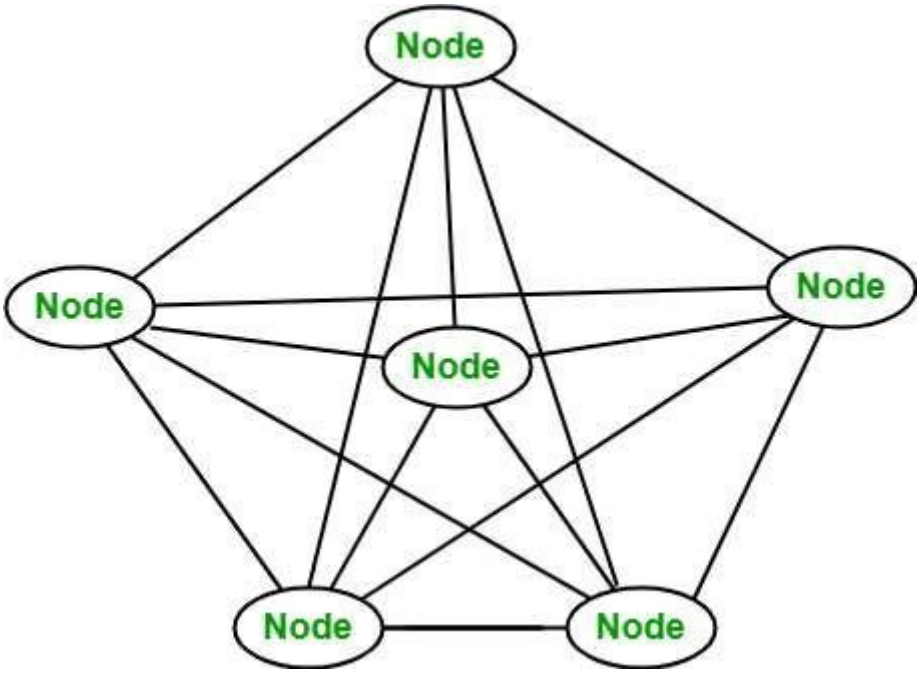

Рисунок 2.7 – Мережа вузлів

Однак, дана конструкція не така масштабована. Саме тому більшість криптовалют в своїй роботі використовують механізм консенсусу на основі лідера. Вузли «суперноди», які відповідають за загальний стан мережі та консенсус обирають дані вузли. Так як дані криптовалюи не є найбільш децентралізованими, то вони є набагато швидшими. Саме тому зараз програмісти шукають найбільш оптимальне рішення, для того щоб досягнути компроміс між швидкістю та децентралізацією.

2.1.3. Недоліки роботи технології Blockchain

Не зважаюси на те, що існує досить багато різних переваг blockchain, існує також багато різних з його прийняттям. Багато перешкод до застосування blockchain не просто технічні, частіше політичні та регуляторні. Проте зі сторони розробників було зроблено багато роботи – тисячі годин, витрачених на розробку програмного забезпечення та backend програмування, які є необхідними для інтеграції blockchain у поточні бізнес-мережі. Деякі недоліки blockchain [9].

- Вартість технології.

  Хоча blockchain заощаджує гроші користувачів на комісіях за транзакції, дана технологія не є дешевою. Наприклад, система Proof of work, яку Bitcoin використовує для перевірки транзакцій, споживає величезну кількість обчислювальної потужності. У реальному світі потужність від мільйонів комп'ютерів у мережі біткойн близко до того, що Данія споживає щорічно. За дослідженням компанії Elite Fixtures, вартість майнінгу одного біткойна різко змінюється залежно від місця розташування комп'ютера - від всього 531 долара до приголомшливих $ 26 170. Проте, майнери отримують за свою роботу перевірки транзакцій набагато більше, ніж віддають за свої рахунки за світло.

- Мала швидкодія

  Системі Proof of work необхідно близько десяти хвилин, для додавання нового блоку в блокчейн. Тому, враховуючи середню швидкість, можна зробити підрахувати, що Bitcoin управляє приблизно сімома операціями в секунду. Інші криптовалюти діють трохи швидше, наприклад, Ethereum – 20 транзакцій в секунду, Bitcoin Cash – 60 транзакцій в секунду. Хоча і швидкодія дещо змінилась, проте дані криптовалюти все ще обмежені blockchain. Для порівняння, Visa обробляє близбко 24000 операцій в секунду.

- Незаконна активність

  Оскільки, дана мережа є конфіденціальною та захищає учасників від злому, це підштовхує досить часто зловмисників до незаконної торгівлі у мережі blockchain. Відомим випадком blockchain для незаконних транзакцій є, напевно, Silk Road, інтернет-ринок «темної павутини», який працював з лютого 2011 року до жовтня 2013 року, доки він не був закритий ФБР. Користувачі Silk Road переглядали сайт, а здійснювали покупки, за допомогою Bitcoin. Американське регулювання запобігає повній

анонімності користувачів онлайн-обмінів, як, наприклад, побудованих на blockchain.

- Проблеми центрального банку

  Кілька центральних банків, включаючи Федеральний резерв, Банк Канади та Банк Англії, розпочали розслідування цифрових валют. Згідно з доповіддю про дослідження Банку Англії від лютого 2015 року, «для подальших досліджень також знадобиться розробити систему, яка могла б використовувати технологію розподіленої книги, не порушуючи можливості центрального банку контролювати свою валюту та захищати систему від системних атак».

- Сприйнятливість до злому

  Нові криптовалюти та блокчейн-мережі піддаються 51% атак. Ці атаки надзвичайно важко здійснити через обчислювальну потужність, необхідну для отримання більшості контролю над блокчейн-мережею, але дослідник інформатики Нью-Йоркського університету Джозеф Бонно сказав, що це може змінитися. У минулому році Бонно випустив звіт, в якому оцінив, що 51% нападів, ймовірно, збільшаться, оскільки хакери тепер можуть просто орендувати обчислювальні сили, а не купувати все обладнання.

2.1.4 . Практичне застосування Blockchain

Слід зауважити, що блоки Blockchain можуть не лише зберігати дані про грошові операції, головним прикладом є кріповалюти, а також і про обмін нерухомості, головування за кандидата і тд [9]. На початку 2020 року було проведено опитування, де з’ясовано, що з тисячі компаній, які розташовано у семи країнах світу, впровадили blockchain близько тридцяти чотирьох відсотків, а сорок один відсоток планували ввести дану систему протягом одного року. Приблизно сорок відсотків наголосили, що наступного року планують інвестувати п’ять, або більше, мільйонів доларів США. Де може використовуватись система blockchain:

- Банківська галузь

  Галузь, яка отримає найбільше позитивних змін від інтеграції blockchain це банківська. Фінансові установи працюють лише 5 днів в неділю, не весь день, тому якщо потрібно виконати якусь операцію в не робочий час, то прийдеться чекати відкриття установи. Крім того, не рідкість такі ситуації, що виконання великих транзакції люди вимушені чекати від одного до трьох днів. Blockchain не має «вихідних». Якщо банки інтегрують blockchain, то користувачі зможуть виконувати транзакції, в не залежності від часу дня та дня тижня, протягом десяти хвилин – це час за який новий блок додається до blockchain. Також blockchain надає можливість банкам безпечнішим способом робити обмін між установами. Процес розрахунків та клірингу у біржовому бізнесі займає приблизно близько трьох днів, або навіть більше, якщо торгівля відбувається на міжнародному ринку, при цьому весь цей час кошти є замороженими. Це є досить ризиковано та банки несуть затрати, протягом даного процесу. Аналітики відомих європейських банків виконали підрахунки та з’ясували, що економія може досягти, близько 20 мільярдів доларів. Дані кошти будуть заощаджені, при використанні технології blockchain, за рахунок страхових та банківських зборів.

- Використання в криптовалюті

  Головним використанням blockchain, так і залишаються криптовалюти, такі як Bitcoin. Центральний орган влади, такий як, банк або уряд регулює та перевіряє валюти, як, наприклад, американський долар. Вартість валюти залежить від багатьох факторів, наприклад, якщо банк працює в країні з нестабільною економікою, то вартість валюти підпадає під загрозу. Біткоїн був створений, саме через дані чинники. Так як, blockchain дозволяє криптовалютам, в тому числі Bitcoin, працювати без необхідності центрального органу, то ризик суттєво зменшується, та дає можливість країні, яка має нестабільну валюту, власну криптовалюту, яка має набагато

ширшу мережу людей та установ, з якими вони можна працювати як на внутрішньому, так і на міжнародному рівні.

- Використання в сфері охорони здоров'я

  Для зберігання медичних записів пацієнтів можна також використовувати blockchain. Коли лікар генерує та підписує медичний запис, він записується до blockchain, це є незмінним доказом. Дані медичні записи можна закодувати та зберегти на blockchain приватним ключем таким чином, що вони були доступними лише певним особам. Цим самим всім пацієнтам буде забезпечена конфіденційність.

- Використання в смарт-контрактах

  Технологія розподіленої книги дозволяє кодувати прості контракти, які виконуються, коли будуть виконані визначені умови. Ethereum - це блокчейн з відкритим кодом, який був побудований спеціально для реалізації цієї можливості. На сучасному рівні розвитку технології, смарт контракти можуть бути запрограмовані на виконання простих функцій. Наприклад, заробітна плата може бути виплачена, коли фінансовий інструмент відповідає певній орієнтиру, використовуючи технологію blockchain та bitcoin, що дозволяє автоматизувати виплату.

2.2. Смарт контракт

Однією з найбільш унікальних особливостей blockchain є її децентралізованість, тобто особливість яка розподіляє права між усіма учасниками мережі, таким чином, виключаючи залучення посередників або сторонніх учасників. Хоча Blockchain має власний набір питань, які ще не вирішені, вони пропонують швидші, дешевші та ефективніші варіанти порівняно з традиційними системами. Завдяки цьому, навіть банки та урядові організації в наші дні звертаються до blockchain.

Смарт-контракти можна назвати як найбільш використане застосування технології blockchain в поточний час. Концепція розумних контрактів була

введена Ніком Сабо, юристом і криптографом у 1994 році [10]. Він дійшов висновку, що будь-яка децентралізована книга може використовуватися як самореалізовані договори, які згодом були названі розумними контрактами. Ці цифрові контракти можна було перетворити в коди і дозволити їх запуск на blockchain.

Хоча ідея розумних контрактів існувала давно, сучасний світ, в якому ми живемо, працює на паперових контрактах. Навіть якщо використовуються цифрові контракти, залучення довіреної сторонньої сторони із системи не може бути усунене. Поки ми визначили систему функціонування цим методом; ми не можемо точно сказати, чи завжди це гладко. Залучення сторонніх осіб може призвести до проблем безпеки або шахрайських дій поряд із збільшенням плати за трансакцію.

З впровадженням технології blockchain в простір цифрових технологій такі питання можна ефективно вирішувати. Система, що базується на технології blockchain, дозволяє всім об'єктам мережі взаємодіяти один з одним розподіленим чином, виключаючи вимогу будь-якої сторони, що довіряється. Простіше кажучи, Blockchain - це технологія, що зберігає дані в розподіленій книзі. Збережені дані записів та транзакцій доступні всім учасникам мережі в режимі реального часу. Технологія Blockchain привернула увагу при впровадженні Bitcoin, першої і найвідомішої криптовалюти на сьогоднішній день. Окрім застосування криптовалюти, Blockchain розвивався і випадки його використання висуваються у різних галузях. Смарт контракти - одне з найуспішніших застосувань технології blockchain. Використання розумних контрактів замість традиційних може значно зменшити трансакційні витрати. Ethereum - найпопулярніша блокчейн-платформа для створення розумних контрактів. Він підтримує функцію під назвою Тьюрінг-повнота, яка дозволяє створювати більш спеціалізовані смарт-контракти. Розумні контракти можуть застосовуватися в різних галузях та сферах, таких як розумні будинки, електронна комерція, управління нерухомістю та активами тощо.

Смарт контракт - це набір комп'ютерного коду між двома або більше сторонами, що працюють на вершині блокчейна, і становить набір правил, узгоджених сторонами (рис. 2.8) [10]. Після виконання, якщо цей набір, заздалегідь визначених правил дотримано, смарт контракт виконує себе для отримання результату. Цей фрагмент коду дозволяє децентралізовану автоматизацію, полегшуючи, перевіряючи та виконуючи умови базової угоди. Смарт-контракти дозволяють обмінювати будь-що цінне, включаючи гроші, акції, майно тощо, прозорим способом, виключаючи необхідність посередника та зберігаючи систему без конфліктів.

Рисунок 2.8 – Схема роботи смарт контракту

У звичайному світовому процесі для отримання документа, зареєстрованого судом, як доказ, вам потрібно буде спершу звернутися до адвоката чи нотаріуса, дати їм гроші в свою чергу за послуги і чекати, поки ви отримаєте необхідний вам документ. Однак сценарій повністю змінюється при смарт-контрактах. Якщо ви запускаєте цей процес за допомогою смарт-контрактів, ви просто отримаєте документ про свою потребу, заплативши

лише це, і це буде зроблено без участі сторонніх осіб, таких як адвокат, у цій справі. Більше того, розумні договори не обмежуються лише визначенням правил навколо будь-якої угоди, але вони також відповідають за автоматичне виконання цих правил та зобов'язань.

Іншими словами, смарт-контракти - це автоматично виконувані рядки коду, які зберігаються на блок-ланцюзі, що містять заздалегідь визначені правила [11]. Коли ці правила виконуються, цей код виконується самостійно і забезпечує вихід. У найпростішій формі смарт-контракти - це програми, які працюють у тому форматі, який їх створив їхній автор. Смарт-контракти є найбільш вигідними у бізнес-співпраці, коли вони використовуються для узгодження вирішених умов, встановлених за згодою обох сторін (рис. 2.9). Це знижує ризик шахрайства, і оскільки в них не задіяно сторонніх, витрати також зменшуються.

Смарт-контракти зазвичай працюють за механізмом, що включає цифрові активи разом із кількома сторонами, де залучені учасники можуть автоматично керувати своїми активами [11]. Ці активи підлягають здачі на зберігання та перерозподіл серед учасників згідно з правилами договору. Смарт-контракти можуть відстежувати ефективність у режимі реального часу та економити витрати.

Властивості смарт-контрактів:

1. самоперевірений.
2. Самостійно виконується.
3. Захищений від несанкціонованого доступу.

Рисунок 2.9 – Принцип роботи смарт-контрактів

Для того, щоб зрозуміти, як працює смарт-контракт, візьмемо приклад, коли людина хоче продати її власність. Процес продажу нерухомості вимагає великої кількості документів, а також спілкування з кількома сторонами. Крім складності спілкування, також можна включати ризик шахрайства. У нинішній час більшість людей, які хочуть мати справу з нерухомістю, ведуть переговори через агентів нерухомості. Ці агенти відповідають за справу з оформленням документів та ринками. Вони виступають посередниками у загальному процесі та працюють над переговорами та наглядовою угодою.

У таких випадках людина не може розраховувати на особу, з якою має справу, тому агенції надають послуги депонування, які перераховують кошти від однієї сторони до іншої. Коли угода буде завершена, особі доведеться заплатити обом, агенту та службі депонування їх комісію в розмірі визначених відсотків. Це призводить до додаткової втрати грошей та більшого ризику для продавця.

Використання смарт-контрактів у таких ситуаціях може призвести до більшої ефективності за рахунок зменшення навантаження. Смарт-контракти

розроблені так, щоб вони працювали за принципом, що ґрунтується на умовах, який вирішить питання власності, передавши його покупцеві лише тоді, коли будуть узгоджені грошові, а також інші умови. Більше того, якщо мова йде про послуги депонування, розумні контракти також можуть замінити їх.

Гроші та право володіння майном можуть зберігатися в розподіленій системі, яку можуть переглядати залучені сторони в режимі реального часу. Оскільки переказ грошей засвідчать усі учасники мережі, шанси на шахрайство усуваються. Більше того, немає жодного шансу залучити посередника, оскільки довіра між сторонами вже не є проблемою. Всі функції, що виконуються агентом з нерухомості, можуть бути закодовані в смарт-контракт, таким чином, заощаджуючи значну суму грошей як покупцеві, так і продавцю.

Застосовуючи смарт-контракти у повсякденному житті, ми можемо внести феноменальні зміни, оскільки вони пропонують численні переваги перед традиційними контрактами. Смарт-контракти є більш зручними та швидшими, що робить їх прийнятними для людей для впорядкування своїх робочих процесів.

Вони надають вам правильну суміш безпеки та простоти застосування, коли потрібно обміняти будь-що цінне, будь то майно, гроші чи спільний доступ.

Усунення потреби в посередниках робить смарт-контракти ще привабливішими для їх застосування в нашому житті. Використання смарт-контрактів, ймовірно, сприятиме прогресу технологій. Переваги, пропоновані смарт-контрактами [11]:

Прозорий

Однією з основних характеристик технології blockchain, яку також мають і смарт-контракти, є прозорість. Як було зазначено раніше, смарт-контракти заповнюються умовами, які детально перевіряються сторонами, що беруть участь в угоді.

Це виключає ймовірність виникнення суперечок та питань на пізніх етапах, оскільки умови ретельно перевіряються та встановлюються лише тоді, коли всі учасники погоджуються з цим. Ця риса смарт-контрактів дозволяє залученим сторонам забезпечити прозорість під час транзакцій.

Більше того, потреба в точності деталізації договору зберігає всю інформацію відкриту для всіх, що врешті-решт вирішує все, що стосується проблеми з комунікаціями. Тому за допомогою смарт-контрактів ефективність, втрачена в прогалинах у спілкуванні, може бути відновлена.

Ефективний у часі

Для того, щоб продовжувати будь-який процес, що включає документацію, зазвичай потрібно більше як мінімум пари днів. Затримка процесів пов'язана з великою кількістю посередників та непотрібними кроками на цьому шляху. З іншого боку, смарт-контракти виконуються за допомогою Інтернету, оскільки вони є не що інше, як програмний код.

Тому швидкість завершення транзакцій за допомогою смарт-кодів занадто швидка. Смарт-контракти можуть заощадити години або навіть дні порівняно з будь-яким традиційним бізнес-процесом. Більше того, затримка часу через ручне залучення також усувається.

Точність

Смарт-контракт кодується у чітко деталізованій формі. Він вимагає утримувати в ньому всі умови, перш ніж нарешті приступить до роботи. Будь-яка умова, яка залишилася поза договором, може призвести до помилки під час виконання, тому під час створення смарт-контрактів усі умови встановлюються у детальній формі.

Завдяки цьому смарт-контракт стає всеосяжною угодою, яка автоматично виконує майже все. Що стосується ручних контрактів, є ймовірність помилок, оскільки особа, відповідальна за укладення договору, може пропустити ту чи іншу умову. Більше того, немає жодного способу навіть відстежити це, поки

помилка не буде зроблена. Тому смарт-контракти є кращою альтернативою для досягнення точності.

- Безпека та ефективність

Смарт-контракти з автоматизованими функціями кодування є найбезпечнішими варіантами, коли мова йде про технологію шифрування даних у поточний час. Оскільки вони відповідають найвищим стандартам безпеки, рівень захисту, що в них бере участь, дозволяє забезпечити їх безпечне використання для критичних процесів.

Зберігання даних

Смарт-контракти точні до найменшого рівня угоди. Усі реквізити будь-якої транзакції зберігаються в договорі, і будь-хто із залучених сторін може отримати доступ до неї в будь-який момент. Більше того, ці транзакції зберігаються на blockchain у вигляді майбутніх записів. Це особливо корисно з точки зору будь-яких суперечок щодо умов контракту в майбутньому.

Економія

Використання смарт-контрактів замість традиційних угод може призвести до значних заощаджень. По-перше, оскільки у смарт-контрактах беруть участь лише сторони, які є частиною угоди; потреба в посередниках усувається, а гроші, що беруть участь у цьому, також заощаджуються.
Усі адвокати, свідки та посередники не грають жодної ролі при використанні смарт-контрактів. Більше того, як було сказано раніше, смарт-контракти також заощаджують гроші, оскільки документи на паперовій основі не залучаються до жодних процесів.

Довіра

Смарт-контракт роблять надійним для бізнесу властивості прозорості та безпеки. Усувається будь-яка ймовірність маніпуляцій, а також помилки, зробленої вручну, та встановлюється впевненість у їх виконанні. Договір автоматично виконує себе після узгодження всіх умов.

Здатність значно зменшити вимоги судових процесів та судів є ще однією унікальною особливістю цих договорів. Смарт-контракт дозволяє сторонам брати на себе зобов’язання та зобов'язуватися за умовами та правилами, записаними всередині, оскільки він виконуються самостійно.

Безпаперовий

Використання паперу у всіх процесах усувається, оскільки смарт-контракти - це документи, кодовані комп'ютером,. З одного боку, це економія витрат, а з іншого - це корисно для компаній у всьому світі, оскільки використання паперу зменшується, за рахунок умов контрактів та це сприяє їх внеску в суспільство.

Застосування смарт-контрактів

Договірні угоди виступають як доказ таких дій, будь-то нова робота або купівля будь-якого нового продукту. Однак високі витрати передбачає складний процес традиційного оформлення документів та контрактів, сторонніх та шанси на помилки вручну в таких процесах.

2.3. Порівняння роботи консенсусів Proof of Work до Proof of Stake

Як вже було написано вище, криптовалюта Ethereum має намір перейти від консенсусу Proof of Work до Proof of Stake [12].

2.3.1. Консенсус Proof of Work

Для того, щоб стримувати різні кібератаки, такі як, наприклад, атака відмови в обслуговуванні (distributed denial-of-service attack (DDoS)), головною задачею якої є вичерпання ресурсів комп'ютерної системи шляхом надсилання декількох підроблених запитів є протокол підтвердження роботи. Ідея концепції Proof of work була опублікована Сінтією Дворк та Моні Наор в 1993 році, а термін був введений Маркусом Якобссоном та Арі Джуелсом у документі, опублікованому в 1999 році [12]. Концепції Proof of work є безпечною та розподіленою, оскільки якщо учасник має намір надіслати або

отримати кошти, йому непотрібно довіряти стороннім послугам, таким як Visa, Mastercard, PayPal, банки, з метою встановлення транзакції . Оскільки вони мають власний реєстр, який зберігає залишки кожного рахунку та веде історію транзакцій, проте при використанні даних послуг, клієнт повинен сплатити комісію. Використовуючи біткоїн або інші криптовалюти, цього робити не потрібно, оскільки кожен учасник має копію blockchain і може самостійно перевірити всю необхідну інформацію.

Тобто, Proof of work – це своєрідна вимога дорогий комп'ютерний розрахунок (майнінг), який виконується для створення нової групи неперевірених транзакцій (блок) на розподіленій книзі (blockchain). Майнінг необхідний для того, щоб [12]:

1. перевірити правильність транзакцій або уникнути подвійного виконання однієї і тієї ж транзакції;
2. створювати нові цифрові валюти шляхом нагородження майнерів за виконання завдання.

Для того, щоб транзакція підтвердилась, виконуються наступні дії:

1. Непідтверджені транзакції збираються у блок.
2. Майнери виконують підтвердження того, що транзакції всередині блоків є законними.

Для виконання попереднього пункту необхідно виконати математичну головоломку, відому як проблема з підтвердженням роботи. Той майнер, який першим вирішить дану проблему кожного з блоків отримає певну винагороду у вигляді, якоїсь кількості одиниць криптовалюти.

3. Транзакції, які пройшли перевірку зберігаються в загальнодоступному blockchain.

Дана "математична головоломка" має ключову особливість: асиметрію. ЇЇ неможливо вирішити інакшим способом, ніж як використанням величезної кількості спроб для знайдення необхідного рішення задачі. В той момент, коли

майнер знайшов правильне рішення, тоді він повідомляє всю мережу про це, та отримує винагороду, яка є передбачена протоколом.

Майнінг – це операція зворотного хешування, тому алгоритм хеш-криптографічних блокових даних призводить до зменшення заданої межі. Даний поріг, який також можна назвати складністю, визначається таким чином: чим більше обчислюваної потужності додається в мережу, тим даний параметр збільшується, як і середня кількість обчислень, які необхідні для створення нового блоку, цим самим збільшуючи його вартість. Це підштовхуючи майнерів до підвищення їх ефективності для підтримки позитивного економічного балансу. Оновлення даного параметру відбувається кожні 14 (чотирнадцять) днів, а новий блок генерується кожні 10 (десять) хвилин.

Проте, зараз Ethereum планує перейти до іншої системи консенсусу, що називається Proof of stake.

2.3.2. Консенсус Proof of stake

Загальний процес залишиться, таким як і в Proof of work, проте сам механізм консенсусу буде повністю віртуальним [12]. У Proof of stake є валідатори, на відміну від Proof of work, в якому майнери вирішують криптографічно важкі головоломки, використовуючи свої обчислювальні ресурси. Валідатори блокують частину свого Ethereum як частку в екосистемі. Потім роблять ставку на блоки, які вони вважають, будуть додані поруч із ланцюжком. Отримуючи винагороду, в залежності від їхньої частки, коли блок буде додано до blockchain.

У розподіленому консенсусі, заснованому на Proof of work, майнерам необхідно багато енергії. Для однієї транзакції з Bitcoin потрібно стільки ж електроенергії, скільки для живлення 1,57 американських домогосподарств протягом одного дня (дані 2019 року). Це призводить по постійного тиску на зменшення криптовалюти, оскільки це оплачується за допомогою фіатних

валют. Вчені, протягом своїх останніх досліджень, з’ясували що операції з Bitcoin споживають стільки ж електроенергії, скільки Данія до 2020 року.
Розробники Ethereum стурбовані цією проблемою, саме тому планує скористатись консенсусом Proof of stake для того, щоб зробити роботу більш економічною та дешевшою, в порівнянні з розподіленим консенсусом Proof of work.

Головним запитанням все ще залишається, чи консенсус Proof of stake безпечніший, ніж консенсус Proof of work? Це особливо важливо, тому що будь-яка комп'ютерна система прагне бути впевненою у відсутності загрози від атак хакерів.

Програмування атаки на консенсус Proof of work є достатньо дорогим, та вкрадене не вартує кількості зусиль та фінансів. Оскільки, консенсус Proof of stake може бути значно дешевшим для атак, тому і потребує максимального захисту.

Для вирішення даної проблеми, розробники Ethereum створили власний протокол CASPER, в основі якого лежить алгоритм ціль якого – встановлення поганого валідатора, використовуючи встановлені раніше обставини. Покаранням буде втрата власного депозиту. Тобто, якщо протокол встановив, що їх дії були неправомірними, порушуючи правила («Умови розсічення»), то подані на початку депозити, буде списано з їх рахунків.

2.3.3. Підсумки порівняння

Отже, завдяки консенсусу Proof of stake валідатори уже не повинні використовувати всю свою обчислювальну потужність, тому що лише кількість власних коштів та поточна складність мережі можуть змінити їх шанси. Тому можна виділити наступні переваги консенсусу Proof of stake відносно консенсусу Proof of work:

- Найбільш важлива перевага -економія енергії.

- Більш безпечна мережа нападів дорожчою. Тобто, якщо зловмисник планував би придбати 51% від загальної кількості фінансів, то ринок відповідно реагує на стрімке підвищення ціни.

Отже, керуючись протоколом CASPER, який базується на системі економічного консенсусу, валідатори повинні сплатити заставу, щоб приймати учать у створенні нових блоків, та саме він буде визначати, яку частину коштів отримає кожен учасник консенсусу, завдяки контролю за депозитами в цінних паперах. Якщо, припустимо, один валідатор створить "недійсний" блок, то депозит буде видалено, а також його привілей бути частиною мережевого консенсусу.

Якщо спробувати перенести дану модель консенсусу Proof of stake на життя, то система безпеки CASPER є досить схожою зі ставками. Можна зробити порівняння, що ставки – транзакції, оскільки саме за них валідатори отримають фінансову винагороду.

Отже, можна зробити підсумок, що під час роботи протоколу Casper валідатори будуть робити ставки відповідно до інших ставок та згодом залишати позитивні відгуки, які здатні прискорити консенсус Proof of stake.

3. СТВОРЕННЯ СМАРТ КОНТРАКТУ ТА ПРИВАТНОГО BLOCKCHAIN

3.1. Створення приватного blockchain

Приватний блокчейн дозволяє лише авторизованим користувачам використовувати мережу blockchain, тим самим регулюючи кількість користувачів всередині мережі, а також контролювати налаштування конфіденційності в мережі, таким чином, щоб жодні дані не оприлюднювалися. Тобто, приватний блокчейн підвищить надійність операцій та безпеку данних користувачів від злочинців.

Для початку розробки приватного blockchain необхідно:

1) встановити geth.

Після всіх необхідних встановлення можна перевірити наявність geth (рис. 3.1).

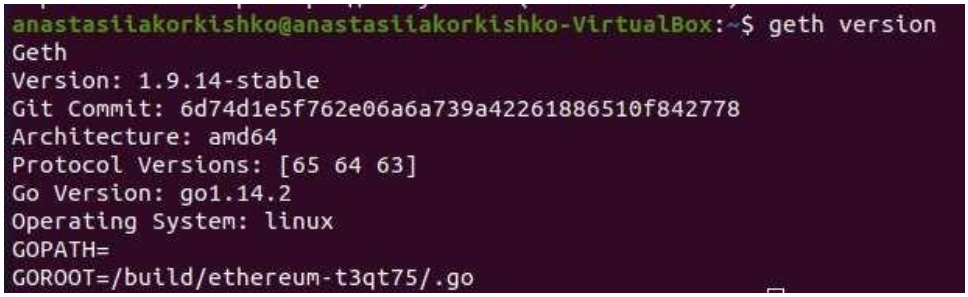

Рисунок 3.1 – Перевірка необхідної версії geth на комп’ютері

Програмне забезпечення Ethereum дозволяє користувачеві налаштувати "приватний" або "тест-мережу" ланцюг Ethereum, який відокремлений від основного ланцюга Ethereum. Це корисно для тестування розподілених додатків, побудованих на Ethereum, без необхідності виставляти власні програми або випробування в реальній мережі Ethereum за допомогою реального Ether.

2) Створення файл генезису

Блок Genesis - це стартовий блок Blockchain - перший блок, блок 0 і єдиний блок, який не вказує на блок попередника. блок генезису важко кодується клієнтам, але в Ethereum це може бути все, що завгодно (рис. 3.2).

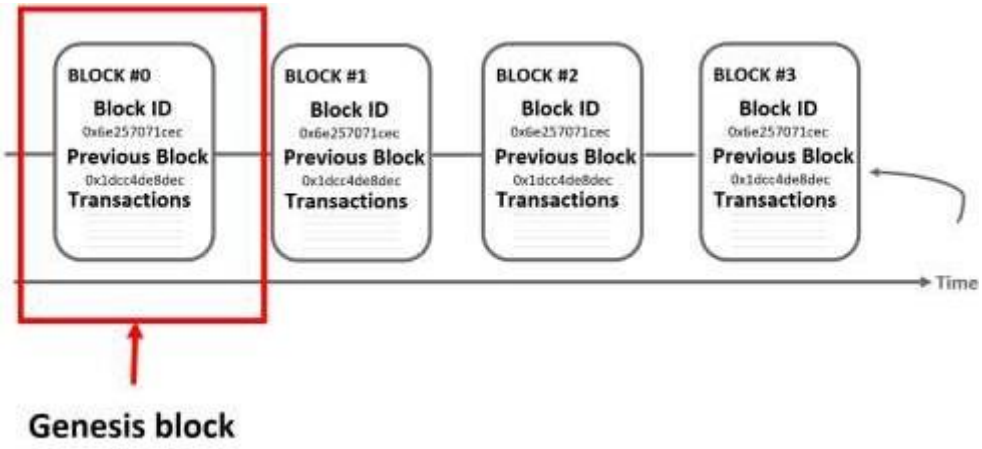

Рисунок 3.2 – Genesis блок в системі блокчейн

Файл Genesis - це файл JSON, який визначає характеристики цього початкового блоку та згодом решти блокчейна (рис. 3.3).

```
{
"config": {
"chainId": 1999,
"homesteadBlock": 0,
"eip150Block": 0,
"eip155Block": 0,
"eip158Block": 0
},
"difficulty": "10",
"gasLimit": "5100000",
"alloc": {}
}
```

Рисунок 3.3 – Вміст файлу genesis

3) Створення акаунту

Після розробки власного blockchain, перш за все спочатку необхідно створити власний акаунт та придумати пароль для входу в нього.

Важливо відзначити, що облікові записи створюються в автономному режимі, і ніхто в мережі не знає адрес / облікових записів, поки вони не будуть включені в транзакцію в мережі.

Отже, для того, щоб мережа дізналася про ці адреси, нам потрібно включити їх у транзакцію та транзакцію в блок (рис. 3.4).

```
INFO [05-25|11:13:03.552] Maximum peer count                       ETH=50 LES=0
 total=50
INFO [05-25|11:13:03.553] Smartcard socket not found, disabling    err="stat /r
un/pcscd/pcscd.comm: no such file or directory"
Your new account is locked with a password. Please give a password. Do not forg
et this password.
Password:
Repeat password:

Your new key was generated

Public address of the key:   0xac723a6406165D409144841FbF4e68cB9BA87a8f
Path of the secret key file: node1/keystore/UTC--2020-05-25T08-13-27.469976508Z
--ac723a6406165d409144841fbf4e68cb9ba87a8f

- You can share your public address with anyone. Others need it to interact wit
h you.
- You must NEVER share the secret key with anyone! The key controls access to y
our funds!
- You must BACKUP your key file! Without the key, it's impossible to access acc
ount funds!
- You must REMEMBER your password! Without the password, it's impossible to dec
rypt the key!
```

Рисунок 3.4 – Створення нового акаунту приватного блокчейну

Внаслідок цього буде згенерована публічна адреса ключа.

Після створення акаунту, необхідно виконати ініціалізацію вузла (рис. 3.5).

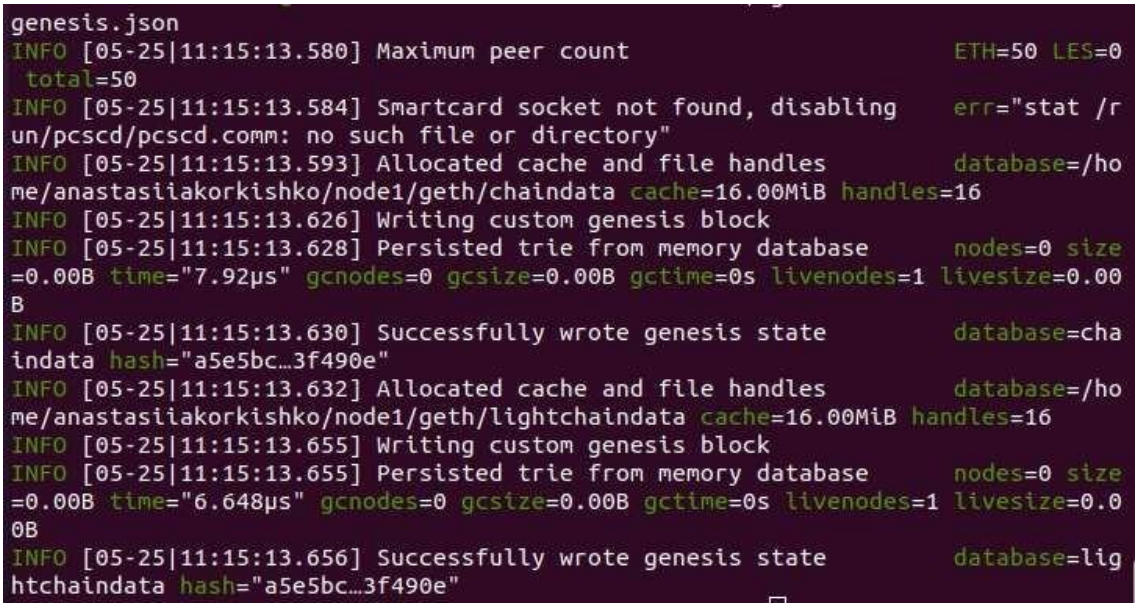

Рисунок 3.5 – Ініціалізація вузла

Після ініціалізації, запускаємо вузол (рис. 3.6).

Рисунок 3.6 – Запуск вузла

Після запуску вузла відкривається консоль Geth, за допомогою якої можна управляти смарт контрактом. Проте спочатку необхідно додати його до даного блокчейну, це можна за допомогою програми Remix, в яку необхідно вставити написаний смарт контракт, та скопіювати його web3 версію (рис. 3.7).

```
WEB3DEPLOY

var crowdsaleContract = web3.eth.contract([{"constant":true,"inputs":[],"name":"totalSupply"
var crowdsale = crowdsaleContract.new(
   {
     from: web3.eth.accounts[0],
     data: '0x60606040525b5b336000806101000a81548173ffffffffffffffffffffffffffffffffffffffff
     gas: '4700000'
   }, function (e, contract){
    console.log(e, contract);
    if (typeof contract.address !== 'undefined') {
         console.log('Contract mined! address: ' + contract.address + ' transactionHash: ' +
    }
})
```

Рисунок 3.7 – web3 версія смарт контракту

Після цього необхідно вставити дану версію в наш приватний блокчейн (рис. 3.8).

```
INFO [05-25|12:08:18.747] Setting new local account                address=0xf3
Dfc5662652Ee50047D04A148326DCA8a1fcDd3
INFO [05-25|12:08:18.748] Submitted contract creation              fullhash=0x9
ba38f500ace7631c2822b006b235d484b902a0f407567a6ce400757fe637366 contract=0x7D57
Ba1FF71be30280337e47FFb1FAcd8abca68b
null [object Object]
INFO [05-25|12:08:18.751] Commit new mining work                   number=1 sea
lhash="50d272…41290c" uncles=0 txs=1 gas=418832 fees=4.18832e-13 elapsed=1.249m
s
undefined
> INFO [05-25|12:08:18.794] Successfully sealed new block           number=1 s
ealhash="50d272…41290c" hash="e57a5f…63650e" elapsed=43.113ms
INFO [05-25|12:08:18.794] 🔨 mined potential block                 number=1 ha
sh="e57a5f…63650e"
INFO [05-25|12:08:18.799] Commit new mining work                   number=2 sea
lhash="012028…5bf249" uncles=0 txs=0 gas=0      fees=0          elapsed=4.241m
s
INFO [05-25|12:08:18.803] Sealing paused, waiting for transactions
INFO [05-25|12:08:18.804] Commit new mining work                   number=2 sea
lhash="012028…5bf249" uncles=0 txs=0 gas=0      fees=0          elapsed=10.010
ms
null [object Object]
Contract mined! address: 0x7d57ba1ff71be30280337e47ffb1facd8abca68b transaction
Hash: 0x9ba38f500ace7631c2822b006b235d484b902a0f407567a6ce400757fe637366
```

Рисунок 3.8 – Опублікування смарт контракту в приватній мережі

Тоді смарт контракт опублікований в приватній мережу. Йому присвоєно адресу. Після цього користувач може звертатися до смарт контракту використовуючи його функції, які будуть описані в наступному розділі.

3.2. Створення смарт контракту

Для написання смарт контракту використовувалась мова Solidity.

Solidity – це високорівнева мова, яка є орієнтованою на контракти та використовується, в основному, для написання смарт контрактів. Blockchain Ethereum, який є розробленим учасниками даної платформи, використовується для повної розробки та втілення смарт контрактів у віртуальну машину Ethereum, або інших платформ для розробки blockchain.

Розробники здатні писати програми, за допомогою високорівневої мови Solidity, та ділової логіки, яка додана до смарт контракту.

Solidity має такі функціональні можливості, на відміну від інших мов програмування на основі віртуальної машини Ethereum:

- Підтримує багатократне успадкування з лінеаризацією C3.
- Підтримка об'єктів або змінних, типів даних та багато інших функцій програмування.
- Складні змінні членів для контракту, який має структури та досить ієрархічне відображення.
- Бінарний інтерфейс програми полегшує декілька функцій безпечного типу в рамках одного контракту.
- Безліч платформ blockchain, включаючи Ethereum, Tendermint, Ethereum Classic, Counterparty та ErisDB, підтримують Solidity.

Solidity підтримує такі типи даних:

1) Цілі числа.

   Solidity може підтримувати як безпідписані, так і підписані цілі домени. Наприклад, такі ключові слова, як "uint256", можна використовувати для виділення розмірів 256 біт, а також підтримують винятки з виконання.

2) Булеві дані.

Булевий тип даних повертає значення "0" як помилкове, а "1" - як істинне, залежно від точності умови. Вихід, як правило, генерується як булеве значення, коли використовуються логічні оператори.

3) Модифікатори.

   Модифікатори використовуються для виявлення відповідності умов до виконання коду смарт-контракту.

4) Строкові літерали.

   Строкові літерали можуть бути представлені подвійними або одинарними лапками.

5) Solidity пропонує переліки, оператори, масиви та хеш-значення для формування структури даних, що називається "відображенням", яка використовується для повернення значень, пов'язаних з місцями зберігання. Оскільки його синтаксис такий же, як у будь-якої загальної мови програмування, він може підтримувати як одно-, так і багатовимірні масиви.

Написаний смарт контракт використовує 0.4.13 версію Solidity (рис. 3.9).

```
pragma solidity ^0.4.13;
```

Рисунок 3.9 – Версія Solidity

Створюється масив з усіма балансами, в якому надалі будуть зберігатися рахунки користувачів (рис. 3.10).

```
mapping (address => uint256) public balanceOf;
mapping (address => mapping (address => uint256)) public allowance;
```

Рисунок 3.10 – Створення масиву

Оголошення публічних змінних нового токену (рис. 3.11).

```
contract token {
    string public standard = 'Token 0.1';
    string public name;
    string public symbol;
    uint8 public decimals;
    uint256 public totalSupply;
```

Рисунок 3.11 – Змінні токену

Функція token ініціалізує контракт з токенами для користувача контракту (рис. 3.12).

```
function token(
    uint256 initialSupply,
    string tokenName,
    uint8 decimalUnits,
    string tokenSymbol
    ){
    balanceOf[msg.sender] = initialSupply;
    totalSupply = initialSupply;
    name = tokenName;
    symbol = tokenSymbol;
    decimals = decimalUnits;
    }
```

Рисунок 3.12 – Реалізація функції token

Функція transfer перевіряє чи відправник має достатню кількість коштів, та перевіряє на переповнення. Потім знімає з балансу відправнику задану кількість коштів, і потім додає стільки ж на рахунок отримувача (рис. 3.13).

```
function transfer(address _to, uint256 _value) {
    if (balanceOf[msg.sender] < _value) throw;
    if (balanceOf[_to] + _value < balanceOf[_to]) throw;
    balanceOf[msg.sender] -= _value;
    balanceOf[_to] += _value;
    Transfer(msg.sender, _to, _value);
}
```

Рисунок 3.13 – Реалізація функції transfer

Функція buy (рис. 3.14) та функція sell (рис. 3.15), які відповідають за продаж та покупку. Спочатку функція buy перевіряє кількість токенів, які можливо купити за допомогою співвідношення msg.value / buyPrice, після цього йде перевірка: чи достатньо грошей для покупки. Після продажу обновляються гаманці продавця та покупця. Функція sell працює схожим чином, тільки зі зворотного боку.

```
function buy() payable {
    uint amount = msg.value / buyPrice;
    if (balanceOf[this] < amount) throw;
    balanceOf[msg.sender] += amount;
    balanceOf[this] -= amount;
    Transfer(this, msg.sender,amount);
}
```

Рисунок 3.14 - Реалізація функції buy

```
function sell(uint256 amount) payable {
    if (balanceOf[msg.sender] < amount) throw;
    balanceOf[this] += amount;
    balanceOf[msg.sender] -= amount;
    if (!msg.sender.send(amount * sellPrice)){
        throw;
    } else {
        Transfer(msg.sender, this, amount);
    }
}
```

Рисунок 3.15 – Реалізація функції sell

Функція setmessage відправляє повідомлення за плату в 1 токен. Для цього спочатку йде перевірка балансу відправника, якщо вміст гаманця більше одиниці, то повідомлення буде відправлено. В іншому випадку, ні (рис. 3.16).

```
function setmessage (string message) payable {
    if (balanceOf[msg.sender] < 1) throw;
    balanceOf[this] += 1;
    balanceOf[msg.sender] -= 1;
    messages = strConcat (messages, ' ', message);
}
```

Рисунок 3.16 - Реалізація функції setmessage

Після цього смарт контракт потрібно завантажити до приватного блокчейну. Випускаємо приблизно 10000 монет токену, який називається LoneCoin (рис. 3.17).

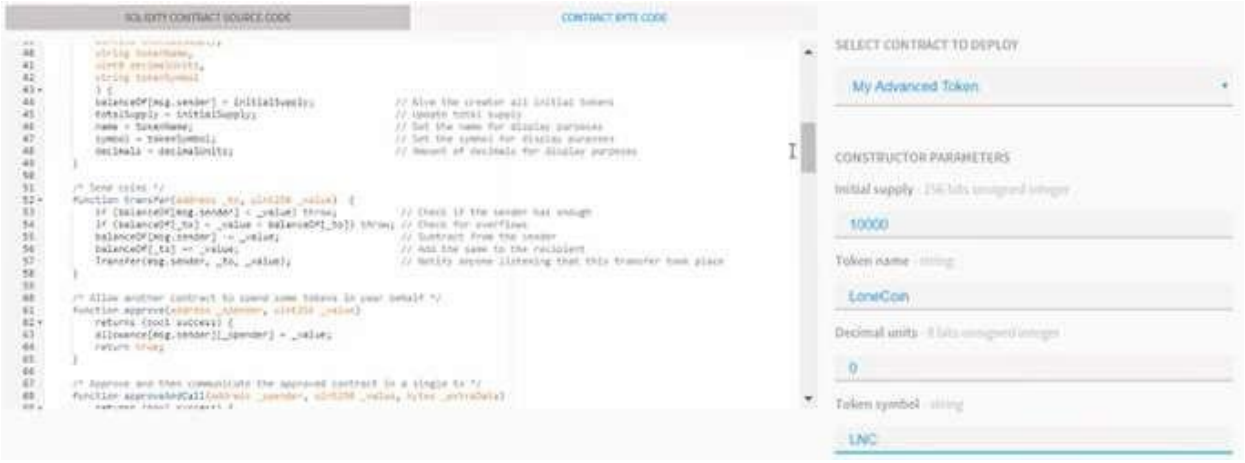

Рисунок 3.17 – Завантаження смарт контракту до приватного блокчейну.

Результат виконання смарт контракту є успішним, тобто можна зробити висновок, що розроблений блокчейн працює правильно (рис. 3.18).

Рисунок 3.18 -Успішне виконання смарт контракту

3.3. Тестування смарт контракту

Смарт контракт – це незмінна програма, тобто після додавання його до блокчейну, змінити його неможливо. Це зроблено для того, щоб дати користувачам впевненість в тому, що правила, якими в подальшому будуть керувати їх грошима, ніхто не зможе змінити. Саме ця особливість робить смарт контракт складним для розробників. Тому тестування є найбільш важливою частиною для смарт контрактів.

Тести допомагають розробнику впевнитися в тому, що всі написані функції працюють так, як потрібно. Також тести допомагають в перевірці функцій на незвичайні моменти, наприклад, що робити, якщо кількість користувачів досягне межі. Такі випадки необхідно враховувати, саме тому тестування є найкращим виходом з даної ситуації.

Для цього розробники написали спеціальну онлайн IDE, яка називається Remix. За допомогою даної програми розробник може протестувати всі функції смарт контракту.

Для цього потрібно відкрити даний сайт та вставити свій смарт контракт та обрати версію Solidity (рис. 3.19). Після цього потрібно скопілювати смарт контракт. Дана онлайн IDE може вказувати користувачеві на попередження та помилки.

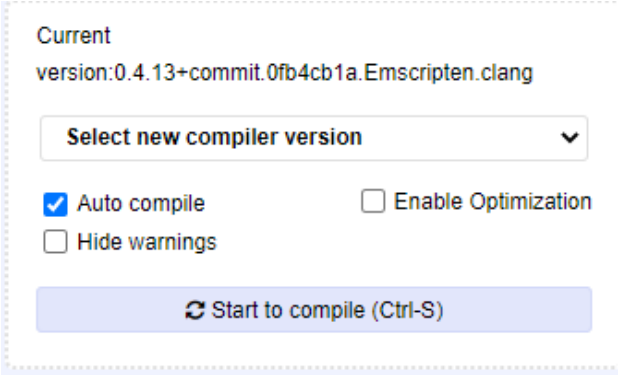

Рисунок 3.19 - Вибір необхідної версії для компілювання смарт контракту

Після цього користувач побачить всі функції смарт контракту, який був завантажений (рис. 3.20).

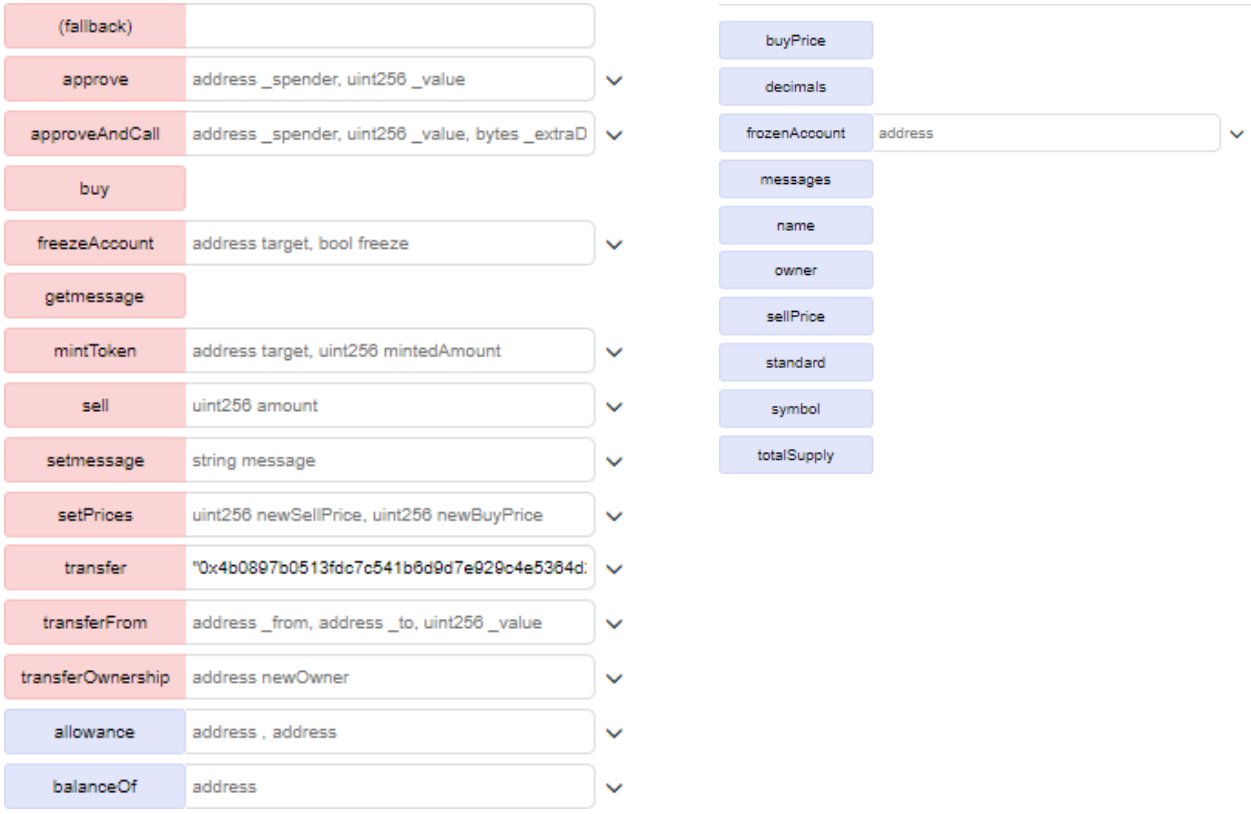

Рисунок 3.20 - Функції смарт контракту, які можна протестувати.

Для проведення тесту можна використати функцію transferFrom, яка містить в собі поля address _from, address _to, uint256 _value (рис. 3.21).

Рисунок 3.21 – Тестування функції transferFrom

Після цього необхідно подивитися баланс рахунку, на який був здійснений переказ за домогою функції balanceOf.

Рисунок 3.22 - Результат переказу

Очевидно, що продемонстрований результат переказу є вірним (рис. 3.22). Після неодноразового тестування всіх зазначених вище функцій зрозуміло, що даний смарт контракт працює правильно.

ВИСНОВКИ

В ході виконання даного дипломного проєкту було проведенно дослідження технології blockchain, смарт контракту, платформи Ethereum, проаналізовано надійність технології blockchain, створено приватний blockchain, розроблено смарт контракт та успішно його протестовано.

У першому розділі було проаналізовано загальний опис проблеми, та як виявилось актуальність проблеми є досить значною. Були розглянуті переваги та недоліки технології blockchain. Як виявилось технологія Blockchain не є досить однозначною, оскільки використання сторонніх платежів робить її досить вразливою, а з іншого боку незворотність транзакцій та багато іншого робить дану технологію з високою надійністю.

Другий розділ дипломного проєкту було повністю присвячено поглибленому розбору роботи технології blockchain, перевагам та недолікам різних принципів роботи, було повністю досліджено смарт контракт та його взаємодію з blockchain та порівняно роботу двох консенсусів Proof of work та Proof of stake.

В третьому розділі було розроблено та створено власний приватний blockchain, написано смарт контракт який взаємодіяв з ним. Протестовано за допомогою програмного забезпечення REMIX та продемонстванно успішну їх роботу.

Задача, яка була поставлена на початку диполомного проєкту, є повністю виконаною та має великий потенціал для подальшого вдосконалення та розвитку. Даний блокчейн та смарт контракт можна використовувати для виконання різноманітних транзакцій.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Blockchain Technology and Its Potential Impact on the Audit and Assurance Profession – [Електронний ресурс]. – Режим доступу: https://www.aicpa.org/content/dam/aicpa/interestareas/frc/assuranceadvisoryservices/downloadabledocuments/.
2. Криптовалюта – [Електронний ресурс]. – Режим доступу: http://www.ereport.ru/articles/finance/kriptovalyuta-prodolzhaet-menyat-mirovuyu-ehkonomiku.htm
3. Биткоин транзакции – [Електронний ресурс]. – Режим доступу: https://ru.bitcoinwiki.org
4. Управление транзакциями в современных реляционных СУБД – [Електронний ресурс]. – Режим доступу: http://web.znu.edu.ua/lab/econom/dba/lectures/ADBS_lect6.pdf
5. Транзакции в сети Биткоин – [Електронний ресурс]. – Режим доступу: https://mining-cryptocurrency.ru/bitcoin-transactions/
6. Надежность биткоина – [Електронний ресурс]. – Режим доступу: https://utmagazine.ru/posts/21428-nadezhnost-bitkoina
7. Свон, Мелани. - Блокчейн: схема новой экономики. — 2018.
8. Лоран Лелу. - Блокчейн от А до Я. Все о технологии десятилетия — 2019.
9. Raval S. - Decentralized Applications. Harnessing Bitcoin's Blockchain Technology. — 2016.
10. Chris Dannen. Introducing Ethereum and Solidity. — Brooklyn, New York, USA: 2017. — 197 с.
11. Iyer K., Dannen C. Building Games with Ethereum Smart Contracts. Intermediate Projects for Solidity Developers. — Brooklyn, New York, USA: 2018. — 281 с.
12. Tromp, John. Financial Cryptography and Data Security: BITCOIN 2015 : journal. — Springer, 2015. — P. 49—62.